OUTSOURCING INFORMATION TECHNOLOGY AND THE INSIDER THREAT

THESIS

Valerie L. Caruso, First Lieutenant, USAF

AFIT/GIR/ENG/03-01

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GIR/ENG/03-01

OUTSOURCING INFORMATION TECHNOLOGY AND THE INSIDER THREAT

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Systems Management

Valerie L. Caruso, BS

First Lieutenant, USAF

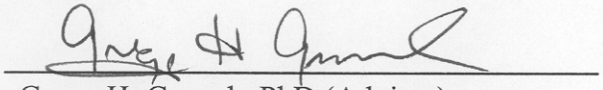
March 2003

AFIT/GIR/ENG/03M-01

OUTSOURCING INFORMATION TECHNOLOGY AND THE INSIDER THREAT

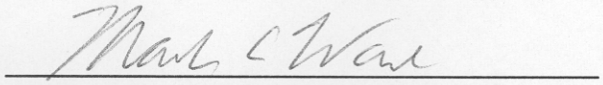
Valerie L. Caruso, BS
First Lieutenant, USAF

Approved:



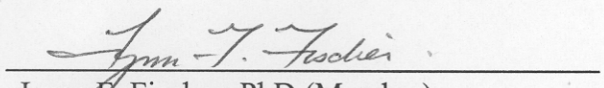
Gregg H. Gunsch, PhD (Advisor)
Assistant Professor of Computer Engineering
Department of Electrical and Computer Engineering

21 Feb03
Date



Mark A. Ward, Maj, USAF (Member)
Assistant Professor of Information Resource Management
Department of Systems and Engineering Management

21 Feb 03
Date



Lynn F. Fischer, PhD (Member)
Social Science Analyst
Defense Personnel Security Research Center (PERSEREC)

21 Feb 03
Date

Acknowledgements

"Every time you don't follow your inner guidance, you feel a loss of energy, loss of power, a sense of spiritual deadness." Shakti Gawain

I'd like to first thank God for blessing me with a life full of wonderful people and experiences – for my health, the ability to serve my country, and opportunities to learn inside and outside the classroom.

Dr. Gunsch, my advisor, I thank you for taking on a stubborn thesis student. You believed in this topic, its relevance, timeliness, and my ability to find a way to present it. My committee members: Major Ward, for guiding my qualitative efforts; and Dr. Fischer for supporting this research from the beginning. I would also like to thank Ms. Hayes and the library technicians for their constant support of my many information requests.

For my family – especially Dad – you've always had faith in me and in my judgment, even when I did not. My beautiful Golden Retriever, Brandon, who made sure I got long walks every morning and evening – ensuring I had a clear head and energy to keep going. My lovely cat, Katie, curled up in my lap while I read, and sat on many papers - keeping me "organized." Both sweet creatures made sure I took time to play and put a smile on my face every day.

Finally, for Mike, my endless source of clarity, motivation, and comfort. You helped me keep everything in perspective, and lifted my spirit – many times. You will have my undying love and respect – always.

Valerie L. Caruso

Table of Contents

Page

List of Figures

List of Tables

Table Page

Abstract

As one of our nation's top critical infrastructures, telecommunications is an essential element of many aspects of our lives upon which we, as a society, are becoming increasingly dependent. Computers, digital telephone switches, and interconnected information technology (IT) systems impact finances, travel, infrastructure management, and missions of national defense.

This research examined whether the trend in increased outsourcing of information technology systems is a significant contributing factor to a reportedly increasing amount of insider attacks. In light of changing social, global economic, and technological conditions, the paradigm in which risk analysis, management practices, and operational and personnel security practices are applied to protect information has shifted over the last decade.

A comprehensive model of the discursive nature of the insider threat in the outsourced IT environment was developed using a qualitative grounded theory approach put forth by Glaser and Strauss in 1967. The theory generated by this research suggests a multidimensional real and growing threat resulting from outsourced IT as well as preconditions for continued future growth of the insider threat phenomenon.

OUTSOURICING INFORMATION TECHNOLOGY AND THE INSIDER THREAT

I. Introduction

Information Technology

The nation's eight critical infrastructures as outlined in Executive Order 13010, which established the President's Commission on Critical Infrastructure Protection, are: “telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.” (Executive Order 13010, 15 July 1996). All of these functions are strongly dependent on information technology (IT).

Recent reports in the government as well as the private sector focusing on information assurance topics specifically mention the insider threat to information, implying the extensiveness and prospective trend in proportional insider threats as a result of increased contracting out of IT functions. This research strove to determine whether existing data supported reported rises in security incidents from the trusted insider. Reports demonstrating the vulnerabilities of sensitive or critical information and associated systems are clear indicators that the insider threat trend is worthy of thorough investigation. Furthermore, this research attempted to increase awareness in the Department of Defense (DoD) and stress the importance of monitoring and managing the insider threat issue to ensure the security of this nation's IT infrastructure and defense-related information systems.

Background

The potential tragedy from ill-meaning insiders with access to sensitive, critical, or classified information, especially with respect to national security and IT infrastructure and systems, is a growing concern in the government. The threat from the inside is now often considered as dangerous (Money, 1999), if not more so than the external intruder (Denning, 1999). However, in this age of contracting out IT, interconnected systems, global economy, and asymmetrical nature of threats imposed by increasing anti-American sentiment, security and the now looming threat of the insider – "protecting information systems from accidental or intentional unauthorized access, disclosure, modification, or destruction" (Loch, 1992, p. 173) may need to be in the forefront of the outsourcing process. This research addressed IT outsourcing from the perspective that the outsourcing trend is growing, and now, more than ever, evidence is pointing to the growing threat of the insider. Outsourcing is traditionally "…motivated by the promise of strategic, economic, and technological benefits" (Lee 1999, p. 36) however, the surety of the IT that permeates business and society must be preserved when considering outsourcing decisions.

Research Question

With the increase in outsourcing Air Force infrastructure operation and maintenance activities (phone switches, communications centers, computer networks) has there been a corresponding increase in malicious insider activity? Has outsourcing and/or use of commercial services in AF information technology contributed to a rise in insider threat-based security incidents?

This topic, especially in light of recent events concerning our national security, is deserving of analysis with respect to insider threat vulnerability. Due to the highly technical nature of the Air Force and the other services it is desirable the results of this research will be generalizable to the entire DoD. Implications for this research apply not only to telephone switches (maintenance, operation, central office, and cable plants) and network control center (NCC) operations, but computer systems involving intelligence, classified, critical mission, personnel, or infrastructure-based data within the Department of Defense.

The specific question to be explored in this research focused on the purported increase in insider-related security incidents since 1990. This time period is chosen for several reasons: the end of the Cold War, force restructuring and military personnel draw-downs, phenomenal growth of the Internet and interconnectivity, global economic expansion of the networked business environment, as well as a noted increase in the outsourcing of government functions. Consequently, has there been a trend in increased insider security incidents in the last decade as a result of outsourcing information technology considered non-core functions?

The IT Outsourcing Trend

The concept of outsourcing technologies and services is not new, and as information technology (IT) continues to permeate nearly every aspect of business (Clark et al., 1995) and society, it can be expected that these services will also succumb to outsourcing practice. In fact, as the complexity and cost of information-based technology continues to increase, the trend to outsource is rising as well (Cheon et al., 1995; Clark et

al., 1995; Klepper and Jones, 1998). Agencies trying to keep up with the latest technologies may not have the ability in-house to provide the high-level IT support necessary to remain competitive.

Examples of IT services subject to outsourcing include: system and network operations and administration, software support, programming, and infrastructure management (Cheon et al., 1995; Antonucci et al., 1998). Proponents of IT outsourcing practice tout the many advantages of contracting out those highly technical services, first and foremost, cost savings and profit.

With the financial aspects of outsourcing being the bottom line for many major management decisions, IT services included, theoretical approaches to this concept have been primarily from an economical standpoint. Private industry and the government practiced outsourcing throughout the 20th century. However, the powerful dynamics of highly technical information systems have dramatically changed the speed, manner, and protocols by which business is accomplished, and these dynamics of technology have imbedded their fundamentals into societal norms. The psychological, social, and organizational implications unaccounted for in traditional outsourcing theory were explored in this research, particularly where modern technology is concerned

The Insider Threat

The insider threat is an emerging topic in information systems literature, however, it was also a major of concern with the nuclear materials management environment in the 1980's. There were 35 Nuclear Materials Management conference papers and journal articles found that were written between 1980 and 1989 that addressed

the emerging threat of the insider. In contrast, there was found only one information technology article during this era - Keough's *Inside Job* Security Management, February 1989, that addressed the insider threat. The point here is the concept of insider threat was being examined as an emerging problem just before the information technology explosion of the decade to follow. It's interesting to note the concerns of the authors such as "…trends in insider activity, the characteristic of the insider, and what actions have been undertaken by the NRC (Nuclear Regulatory Commission) and some of our licensees to counter the insider threat" (Quinn, E.A., 1983). Another well-published author on the subject states, "… attention is shifting toward achieving comparable protection against insiders. Since threats and protection measures for insiders are substantially different from those for outsiders, new perspectives and approaches are needed" (Al-Ayat et al., 1986). The protection concerns of nuclear materials from insider threats during the era of nuclear proliferation parallel today's threats from the insider during an age of potential information warfare. The warfare tactics and the associated literature domains may have shifted focus, however, the original threat from the insider is still a phenomenon worthy of examination.

Meet the Insider

In her 1999 book titled Information Warfare and Security, computer security expert Dr. Dorothy Denning, dedicates an entire chapter, named "Behind the Fence," to the gravity of the internal threat. This chapter begins with the following statement:

> Insiders - employees and others in trusted positions within or with an organization - are generally regarded as the greatest threat to an organization's information resources. This is not surprising, as they have the greatest access to information

within the organization. They could exploit information resources for personal gain or sabotage computer systems for revenge. They could unintentionally reveal secrets to contractors, partners, customers, or outsiders requesting information. (p.131)

Other definitions of insider with respect to information technology:

- "Anyone who is or has been authorized access to a DoD information system whether a military member, a DoD civilian employee, or employee of another Federal agency or the private Sector" (IPT, 2000, p. 3).

- "Employees, contractors, service providers, or anyone with legitimate access to a system. All insiders have some degree of physical or administrative access to IS [information systems]. The greater the individual's knowledge of and access to the system, the greater the potential threat from that person, with individuals having privileged access posing the greatest potential threat" (NTISSC, 1999).

- "Include not only employees (current, former, or temporary) of the computer owner but also persons providing software (e.g. suppliers) and maintenance services to the systems (e.g. consultant or independent contractors)" (Zaiton, 2000, p. 106).

The Risk

Outsourcing IT risks that have been addressed in literature include: loss of control and flexibility (Lacity et al., 1995; Antonucci et al., 1998; Tayntor, 2001); costs (Clark et al., 1995; Grover et al., 1996; Antonucci et al., 1998); service quality (Grover et al., 1996; Klepper and Jones, 1998); and technological or competitive advantage (Cheon et al., 1995; Clark et al., 1995). As the outsourcing trend increases (Clark et al., 1995; Klepper and Jones, 1998; Sambamurthy and Zmud, 2000; Sherwood, 1997), and IT becomes more critical to business and society as a whole (Magklaras and Furnell, 2002), it is a logical assumption that the insider threat will increase as more outsiders gain inside access to an organization's information and associated technology. This risk has been

underestimated and only until recently (late 1990s) has literature begun discussing the insider threat as a growing concern in outsourced IT.

There existed further opportunities and justification to investigate with increased scrutiny the risk the insider threat poses to system security as the outsourcing trend continues to increase. Risk analysis should play a tremendous role as society becomes more conscious of security. Placing quantitative values on information resources or considering transaction costs of strengthening corporate information assurance programs will more likely become more commonplace in decision analysis of IT outsourcing. Dieter Fink attempted to present a framework for examining "loss of security and control when IS [information systems] outsourcing occurs…" (1994, p. 3) and addressed levels of controls and other necessary considerations that if ignored, could have possibly irreversible and costly impacts on core processes, resources, and finances. He further states the simple fact that "…a major concern of the vendor is processing efficiency (maximizing output and minimizing costs) while for the client it is systems integrity. Controls for the latter add overhead to information processing" (1994, p. 7).

Even when a company has controls in place, sometimes the risks are unavoidable. A disturbing notion is generated by an annual survey accomplished by the Computer Security Institute and the FBI, now in its seventh year. After surveying over 500 computer security specialists each year, it was concluded that an alarming number of the unauthorized access and misuse incidents detected were from insiders: 40 percent in 1997; 44 percent in 1998; 55 percent in 1999; 71 percent in 2000; 49 percent in 2001; and 38 percent in 2002 (Power, 2002). Furthermore, a recent Project on Government Oversight (POGO) report on the top grossing government technology contractors stated,

"the government continues to do business with companies that repeatedly violate the laws and regulations…" (2002, p. 4). Therefore, if it is now known that our some of our most frequently used, highly technical contractors have been historically misleading the government, is it illogical to assume that contracting out something as critical as IT may not place the DoD's information and infrastructure in the most secure hands?

According to a recent Office of Management and Budget (OMB) report:

> DoD has conducted the largest competitive sourcing program in the federal government, and is planning to compete 15 percent of those positions not deemed inherently governmental by 2003. Competitions are spread out over a wide array of military base functions, including communications, computing, and maintenance and repair. (OMB, 2002, p.8)

Without regard for the law how important is security policy to the companies landing high-dollar contracts? There are many questions motivating this research and a strong belief that there is evidence the insider threat (contracted and otherwise) is real, and is increasing in the DoD.

Scope of this Research

This research focused on the insider threat with respect to information technology that is contracted out by the DoD. By studying any data that was made available over the past 10 to 12 years that could have possibly helped determine whether there is a trend in rising security incidents from the inside, it generated valuable recommendations that may help refine government acquisition, personnel security, and operational procedures to ensure information systems and infrastructure are not at an increased risk for sabotage, infiltration, or compromise.

Summary

This chapter introduces a hypothesized relationship between the insider threat and the outsourcing trend. It gives an overview of theorized justification to aggressively confront the current threats to DoD information technology with respect to today's asymmetrical warfare realities. Finally, by analyzing outsourcing philosophy, the trend in outsourcing information technology, and the growing evidence of the insider threat, Chapter One is the foundation for this research endeavor.

Chapter Two covers related work and research domains impacting outsourcing and the associated insider threat, as well as how this research differs from previously existing work. Chapter Three defines the research methodology and discusses how this thesis addresses a relationship between an increase in outsourcing and increased insider threat security incidents. Chapter Four presents an analysis of available data for this research and summarizes the results of the study. Chapter Five examines the model and emerged theory while comparing against an actual high-profile insider threat case. Finally, Chapter Six provides a conclusion and presents recommendations and possibilities for future work in this area.

II. Literature Review

Introduction

Little peer-reviewed literature addresses the insider threat, especially with respect to outsourcing. However, due to the timeliness and relevancy of this topic in modern Information Technology (IT) culture, literature from related fields was reviewed. What emerged was a comprehensive data mine of theory, cases, testimony, and literature that gave this research a rich, multidimensional perspective from which the insider threat can be studied.

Insider Threat Trend in Literature

Common occurrences were noted in the existing, limited literature referring to aspects of the insider threat (human, computer use, or general threat-based) and indicated that the insider threat situation was either the most significant threat facing today's information systems, or an increasing problem. An initial analysis was performed to see what data was actually provoking the impression that the insider threat was, indeed, increasing. It was interesting to find that many sources based their statements on one primary source of reference, which is the Annual FBI/CSI Survey, now in its 7th year.

Schultz (2002) points out in *A Framework for Understanding and Predicting Insider Attacks*: in spite of the "belief that 'most attacks come from the inside' …empirical statistics and firewall logs show otherwise" (p. 1).

Table 1 summarizes references to the severity or increasing trend in insider threat, based on the statistical information put forth in the annual survey.

Table 1: Literary References to Insider Threat Trends

Reference	Year	Increasing Threat	Greatest/Most Serious Threat
Peters, 1999	1997, 1998	"Defense officials are increasingly concerned about trusted employees seeking restricted data." "We are increasingly concerned about those who have legitimate access to our networks – the trusted insider"	"I cannot emphasize strongly enough the seriousness of the insider threat to our information systems, and through those systems, our department's operations" (Quote in the article by Deputy Defense Secretary John Hamre).
NTISSC, 1999	1998	"The modern trend of outsourcing and the use of Commercial-off-the-Shelf (COTS) products have dramatically expanded the pool of insiders, giving third parties access to hardware and software at many lifecycle points."	"While government IS face a variety of threats from a variety of sources, the greatest potential threat comes from insiders with legitimate access to those systems."
Zaiton, 2000	1998	"Despite increase in the threat to computer systems from external hackers, particularly the internet, insiders provide the other likely source of threat, which suggest that there is a general trend of increasing in harm both from outside of an organization as well as from within." "Unauthorized modification or deletion of data or causing damage to the organization computer network is one of the alarming trends of the insider cyber vandalism which is becoming a concern for organizations."	"Insiders pose enormous legal dilemmas for their employers who have to decide how to deal with threats or harm arising from computer misuse." "Insider threats, which are not new, have a considerable potential scale of harm and wide ranging implications…may not only affect the operational efficiency of the company's computer system as a whole, but may also threaten the existence of the organization."
NCS, 2000	1999, 2000	"The technological, economic, and social conditions that have led to today's business environment are likely to persist, increasing the insider threat and posing new challenges for corporate and government security professionals."	"Because they are familiar with the organization, malicious insiders have a greater opportunity to do harm than outsiders."
FBI, 2000	2000	"More companies are reporting intrusions."	"Disgruntled insider is principle source of computer crimes."
Magklaras and Furnell, 2002	2001	"Well documented emerging insider threat."	"Insiders constitute greater level of threat than outsiders because of the greater level of knowledge they possess about critical components of the IT infrastructure."

This research is not intended by any means to discount the merit of the FBI/CSI survey. In fact, "While some researchers warn that survey data on computer crimes can be inaccurate due to unreported or undetected acts, such data are useful in characterizing a minimum level of threat and in drawing attention to the problem as a whole" (Shaw et al., 1998, p. 3). This survey has become a consistent contribution to the practitioner's body of knowledge and a constant indicator that the threat is significant and should continue to be addressed at all levels of an organization. Furthermore, according to research performed for the OASD/C3I by Political Psychology Associates, Ltd., "Overall, case investigators report that the number of computer-related offenses committed by insiders is rising rapidly each year" (Shaw et al., 1998). This trend was reported while the FBI/CSI survey was in its second year. There exist cases clearly demonstrating the gravity of the insider threat, however, in the last two years of the surveys, the inside intrusions seem to be decreasing, as shown in the following table:

Table 2: Insider Threat Percentages (Power, 2002)

Year of Survey	Percentage Incidents from Insiders
1997	40
1998	44
1999	55
2000	71
2001	49
2002	38

The decrease after the year 2000 in the percentage of insider incidents could possibly be explained several ways: the proportion of attacks from the outside is increasing; insider incidents are not being reported due to perceived risk of appearing to have poor security programs or bad publicity; or more insiders are remaining undetected (Shaw et al., 1998).

Therefore, while the primary research area is the insider threat, the literature reviewed in the next few sections will focus on information technology environment forged by events or conditions such as outsourcing, psychology of the information technology professional, and the global IT environment and resulting social and economic manifestations. Their hypothesized relationships to the core category were prospected by their impact on the insider threat concept. The integration of the properties for each category is intended to show the driving force behind the perceived increasing insider threat to IT within the DoD.

Outsourcing Theory

"The predominant reason for outsourcing is to cut operating costs and improve efficiency" (Jurison, 1995, p. 239). Outsourcing theory, as it applies to IT, has been studied from mainly economic and strategic management-perspectives, which will be the main focus of this section. There has been some examination of IT outsourcing from the social perspective as well, however, it is less prolific. And while outsourcing theory has been applied successfully in the past, present day technology brings with it threats that may not comprehensively considered by these theories.

Outsourcing Decisions

There are several theoretical approaches to evaluating outsourcing decisions that have roots in economic, strategic management, decision and social science areas of study. The economic perspectives found to be most common in literature on outsourcing IT are the theories focusing on the transaction and agency costs. Among the most commonly found strategic management perspectives are the theories pertaining to resource based decisions strategies and the dependency of organizations on others for resources.

Social Theories

Theories used to study outsourcing from a social perspective include social exchange, social contract, and power-political theories. However, due to limited literature focusing on the social theories that relate specifically to the outsourcing of IT, and the scope and time constraints, this review will cover the more commonly studied theories. Social theories have been grounded in other fields of study, such as economics, psychology, and sociology (Sun, Lin, and Sun, 2002) and are important, however to the insider threat concept. Psychological and social science perspectives such as include trust, employee loyalty (commitment) and psychological contracts are extremely relevant to this study, and were included in this research.

Economic Theories

Cost-based outsourcing philosophy accommodates theory based on the belief that organizations can lower their production costs by contracting out production-oriented tasks to vendors who may be able to perform the labor at a rate that would essentially save an agency money (Grover et al., 1996; Klepper and Jones, 1998). However, for

outsourcing to be successful "…the costs of negotiating a contract with a vendor, managing the vendor relationship, and making sure the vendor does what the vendor has contracted to do…" or transaction costs must not exceed the company's prospective gain (Klepper and Jones, 1998, p. 54).

The government is no different when it comes to economic strategy. Government outsourcing practices can be considered a blend of economic and strategic based strategies. Office of Management and Budget (OMB) Circular Number (No.) A-76 lays out government policy for fostering fair and open competition among civilian product and service suppliers to the government. OMB Circular No. A-76 is a basis for sound economics for government spending. By examining the background and general philosophies behind outsourcing theory, the reader will gain insight into the economic and strategic management theories that have long been the foundation for past and present day outsourcing decisions (Levina, 1999). However, these theories may be considerably outdated in present and future conditions requiring more attention to security as a priority in the outsourcing decision-making process.

Two theoretical models commonly referenced in literature are used to understand and evaluate outsourcing decisions. These are the Transaction Cost Theory (TCT), originally founded by R.H. Coase in 1937 (Cheon et al., 1995; Clemons et al., 1993), and the Agency Cost Theory (ACT), proposed by S. Ross in 1973 (Cheon et al., 1995). Both perspectives have their origins in the economic areas of study and have been a focus of evaluation as to their appropriateness of outsourcing (Willcocks et al., 1995). Upon closer observation of the two models, it should be clear management decisions to

outsource information technology and its intricacies may not be comprehensively evaluated by these primarily financially-oriented models.

Transaction Cost Theory (TCT)

TCT is a classic model developed more progressively by O. Williamson (Cheon et al., 1995; Clark et al., 1995; Clemons et al., 1993; Willcocks et al., 1995). Cheon, Grover, and Teng present the TCT as it applies to their outsourcing perspectives and subsequent contingency theory model. They address the factors to which higher transaction costs may be attributed: asset specificity, technology and skills unique to a company; uncertainty, driven by market, technology, or economic behavior or trends; and infrequency of contracting, brought about by newly-developed vendor relationships. The primary focus of the TCT model is the economic efficiency of the production-oriented organization (1995). Slaughter and Ang also observed trends toward cost-based outsourcing as reactions to technological and environmental uncertainties (1996). The emerging risk of internal threat is not mentioned specifically, as literature is only beginning to address this reality.

Agency Cost Theory (ACT)

The second economic theory gives more insight to risk assessment when facing the difficult management decision of whether to outsource information technology. The Agency Cost Theory (ACT), although not as rigorously studied throughout literature as the TCT, focuses more on the relationships between the company and the contracted individual vendor. Like the TCT and the evaluation of proposed transaction costs, under ACT the agency costs are evaluated; if these costs project a financial savings based on expected gain, outsourcing IT is considered a wise management strategy.

The ACT, however, gives a broader perspective of possible risks a company may encounter, as it observes contributing factors (similar to the TCT's three transaction cost factors) that could impact agency costs. This theory also takes into account uncertainties much like the TCT, but differs in that it directly addresses risk aversion. However, the insider threat to information systems and infrastructure is not adequately considered. Other factors include: predetermined programmability, if possible, of the service provider; possible measurement of future contract outcomes; and the length of the agreement (Cheon et al., 1995).

Strategic Management Theories

The remaining two theories that were reviewed are the Resource-Based Theory (RBT) and Resource-Dependence Theory (RDT) that originated in the strategic management field of study (Cheon et al., 1995). They are not studied as intensely as the TCT, but give a more asset-based perspective on outsourcing of IT, so they will be examined briefly to ensure a well-rounded theoretical perspective.

Resource Based Theory (RBT)

RBT philosophy centers on a thorough review of a company's resources (mainly firm capital) and outsourcing accordingly, in order to fill gaps in management strategies not satisfied by existing resources (Cheon et al., 1995; Klepper and Jones, 1998). Strategic management theory appears to review assets and capabilities and may be more applicable to IT outsourcing strategy. Cheon, Grover, and Teng provide an in-depth analysis of RBT and its constructs. They relate to resource specifics, such as uniqueness (also noted in ACT), and the ability to not only fill gaps in the existing resource base, but

to pull in new capabilities that keep the organization competitive and aligned with its strategic goals (1995).

Other perspective views IT functions and innovation as a source of competitive advantage for an organization (Mata and Fuerst, 1995; Claver et al., 1998). Proprietary technology and some technical and managerial skills are examples of valuable IT assets from a resource-based perspective. A manager's "ability to conceive of, develop, and exploit IT applications to support and enhance other business functions" (Mata and Fuerst, 1995, p. 498) would place a company in a competitively advantageous position. Mata and Fuerst conclude that it is IT managerial skills that "are likely to be a source of sustained competitive advantage" (p. 499).

Technological innovation can be considered a resource if the organizational culture is immersed in "innovative attitude" which must be present for successful technological development (Claver et al., 1998).

Resource Dependency Theory (RDT)

The second of the strategic management class of outsourcing theory, Resource-Dependence Theory, dictates that all companies must inevitably obtain resources from outside their organizations (Cheon et al., 1995; Klepper and Jones, 1998). Lacity, Willcocks, and Feeney declared a trend in management attitude to automatically outsource highly technical tasks because "…no one in the company has enough technical expertise to assess new technologies, they should hand the job over to an outsider" (1995, p. 91). The basis of this theory, according to Cheon, Grover, and Teng "…emphasizes the dependence of organizations on their external environment, provides a useful

perspective from which to examine the relationship between an organization's decision to outsource IS functions and that organization's effectiveness" (1995, p. 213).

Review of the historical value of outsourcing theory as it applies to the modern day information technology environment led to a presumption that economic and strategic management practices do not often have the security interests and risk considerations of the systems at the forefront of the contracting process. It is believed the threats are inadequately addressed by theories developed in the early part of the last century before computers and interconnected systems were a vital part of business practice. Although a prominent roadmap from prospective outsourcing decision, the risks encountered by modern day information technology complicate the outsourcing process on many levels – including the human level. Slaughter and Ang (1995) recognized the implications of outsourcing could have social and psychological effects on an organization's workers. The human factors are examined in the next section.

Insider Threat – Psychological and Social Perspectives

Familiarization of classic outsourcing theories with respect to risk analysis makes it necessary to also investigate characteristics of the information technology environment that relate to the socioeconomic and psychological realms. A significant portion of the risk that an organization entails can be attributed to the human factor. Often, this may be overlooked in the efforts to increase economic or technological advantages, however, literature is pointing toward evidence that if personnel security management is not a priority, outsourcing efforts may end up costing more in the long run.

Profile of Information Technology Professional

Existing literature by Shaw, Ruby, and Post of George Washington University, and Heuer of the Defense Personnel Security Research Center (PERSEREC) identify a perceivably introverted characteristic of typical IT professionals. Psychologists believe this primary personality trait of information technology professionals is a probable source of malicious activity from the inside - especially in the case of the disgruntled IT professional. The personality trait found to be common among analyzed computer professionals was that of introversion (Shaw et al., 1999).

There are several reasons for concern regarding the introverted computer specialist. Introverted computer professionals often relate better to computers than people, and become easily frustrated and less tolerant to stress. Because of inadequate skills to communicate effectively, their problems with the organization, boss, or other employees are often manifested in the form of computer-based attacks. The personality traits of the modern computer technology professional are found to "...create an increased vulnerability to feelings of alienation, disgruntlement and disappointment on the job" (Shaw et al., 1999).

The loyalty of the IT professional to a particular company has come under question in literature as computer technology professionals are being paid sometimes exorbitant amounts for their skills, and some companies are looking to hire former computer hackers. This mentality, fostered by a narcissistic nature, suggests IT employees are more prone to seeking revenge if not treated like (or monetarily compensated for) the special, talented, and gifted employees they believe themselves to be (Shaw et al., 1999).

A recent, blatant example of failing loyalty due to this narcissistic nature is the case of a TRW contractor, Brian Regan, who felt that he was worth more for his years of service and expertise in intelligence analysis systems than he was being paid. In an attempt to seek revenge for perceived inadequate compensation for his services, Regan contacted a leader of an adversarial nation to the United States and offered classified intelligence information in return for 13 million dollars. The letter to Sadam Hussein is reproduced in the Superceding Indictment filed 14 February 2002 and states, "I have been with the CIA for over twenty years and I will be retiring in two years. I feel that I deserve more than the small pension I will recive [sic] for all the years of service at the CIA" (McNulty, 2002, p. 8).

Employee loyalty factors are believed to be cogent contributors to security issues of the information technology environment. Employee loyalty is a multi-dimensional interest where IT is concerned, due to not only the introverted, narcissistic nature if the IT professional, but the nature of temporary or contracted employees, as well as employees of non-U.S. born origin. These factors are examined in the following sections.

Employee Loyalty

There are several theories behind why an employee would consider stealing, sabotaging, or destroying company information, or abusing information technology. First, there is the belief that there are certain psychological profiles typical of information technology professional, as outlined in the previous section. Inherent traits that foster illicit behavior, as well as sociological determinants are also believed to be the result of increasing downsizing, outsourcing, hiring of more qualified personnel of non-US born

origin, or the trend toward short term versus long term employment (Heuer, 1999). A more simplified approach associated with profit or respect or power (derived from hacker-based mentality) has also been proposed. All of these possible causes can be related to the outsourcing trend as IT functions are contracted out to none other than hard-core IT specialists.

Hodson and Sullivan of the University of Texas propose employee loyalty is based on "intended continuance and perceived job status" (1985, p. 719). When applying outsourcing philosophy to an employment situation that involves contractor employees or a pending contracting-out situations, one can observe a possibly significant source of employee disloyalty. There are numerous documented cases of contractor personnel wreaking havoc on a company once they knew their contract was being terminated or they were being relieved of duty for other reasons.

In 1998, in a statement on Threats to the U.S. National Security, Louis J. Freeh, Director, FBI, addressed the Senate Select Committee on Intelligence. In this statement he reports, "A large portion of the computer intrusion reports that the FBI and other law enforcement organizations receive have at their core an employee, or a former employee, who has exceeded his or her access, often in revenge for a perceived offense or wrong" (FBI, 1998, p. 12).

Increased foreign influence and growing anti-American sentiment

There are reasons to infer the increased risk to insider threats based on social and economic changes in America and our relationship with other nations. According to

Heuer (2001), there are several factors leading to this belief that the security of inside information is increasingly at risk due to foreign influence:

> About half of all the doctoral degrees in physics, chemistry and computer science granted by U.S. universities now go to foreign-born students. One-third of all engineers in Silicon Valley were foreign born. This increasing internationalization of many high technology fields, combined with the increased number and variety of countries conducting intelligence operations against the United States, may increase the prevalence of conflicting loyalties. (p. 3)

While foreign-owned U.S. companies have been awarded highly sensitive or classified contracts for software development and communications systems (such as the DoD's Worldwide Military Command and Control System (WWMCCS) (USGA, 1996) there are reasons to infer the risk to critical systems from the inside could be increasing as well.

Systemic Review

In an age of downsizing and retention issues the government has also taken economic and asset-based approaches to its outsourcing practices. OMB Circular No. A-76 addresses this in paragraph 5 of its stated policy to "Achieve Economy and enhance Productivity, Retain [inherently] Governmental Functions In-House, and Rely on the Commercial Sector" (1999). Faced with competitive sourcing targets of "15 percent of all federal jobs considered commercial in nature by the end of fiscal 2003" (Peckenpaugh, 2002, p. 1), the DoD faces the challenge of balancing OMB directives with mission requirements and national security objectives. For a job to be considered commercial in nature, it would have to not be inherently governmental. According to Peckenpaugh (2001):

> The definition of inherently governmental work dates to 1966, when the old Bureau of the Budget issued Circular A-76. The circular defined inherently governmental functions as being "so intimately related to the public interest as to mandate performance by federal employees." This general definition was adopted by the Office of Federal Procurement Policy (OFPP) in its 1992 review and by Congress in the 1998 Federal Activities Inventory Reform (FAIR) act. (p. 2)

Amidst changing DoD transformational strategies, it is becoming less clear whether Information Superiority objectives can be effectively met through outsourcing IT functions. This section reviews the systemic facets of the personnel, security, and computer security relevant to outsourcing IT. It presents a temporal synopsis of the progress and published efforts within the federal government to address the insider threat element since the Cold War era. Historical information and reports published by federal government offices addressing issues appurtenant to personnel security reviews of contractor personnel, malicious acts from trusted insiders, inefficient security controls for contractors, as well as the ever-present foreign interest and espionage concerns were the foundation for this information review.

Personnel Screening

According to a congressional memorandum addressing a March 2, 2001 hearing in which a Subcommittee on National Security examined the security clearance investigation backlog, the GAO estimated "the DSS personnel security investigations backlog for defense, civilian and contractor personnel was approximately 505,000 cases, and growing…However, the actual size of the backlog is unknown because DoD and military personnel databases cannot provide an accurate count of clearances requested or overdue" (DSS, 2001, p. 6).

For those unclassified systems, innumerable contractors and subcontractors continue to be entrusted with defense technology, information, and infrastructure where no definitive screening process currently exists. Shaw, Ruby, and Post found in their study that:

> Many organizations within the critical infrastructure but outside the intelligence community have little control over the pre-employment procedures and hiring practices utilized by the contractor or consulting group. This is true even though contractors and consultants (and sometimes temps) often have highly privileged access to the organization's information assets due to the increased outsourcing of programming and other information technology functions. (1998, p. 5)

In his Annual Report to the President and the Congress, Secretary of Defense Donald Rumsfeld addressed insider threat vulnerabilities:

> Transforming the screening processes and reviews to reduce the backlog of clearance investigations, conducting vulnerability assessments of critical assets, increasing support to counterintelligence and industrial security, as well as leveraging technology are key thrusts. (2002, p. 101)

Contractor Trust

A Project on Government Oversight (POGO) report in 2002 reveals that:

> The federal government continues to do business with companies that repeatedly violate laws and regulations, despite rules specifying that 'Purchases will be made from, and contracts shall be awarded to, responsible contractors only. To be determined responsible, a prospective contractor must have a satisfactory record of integrity and business ethics' (Federal Acquisition Regulation (FAR) 9.103(a)). (POGO, 2002, p.4)

Between 1990 and 2002, 43 of the top defense contractors have pled guilty to or settled such charges as:

- "concealment of commissions paid to consultants who helped obtain contracts to obtain military sales to foreign governments ... ."

- "the information transferred [to the Chinese Government] was inappropriate ... and ... there was a serious problem here that information had the potential to be used to be applied to missile development."

- "Digital Equipment Corporation, which Compaq purchased in 1998, [allegedly] inflated its labor costs on a Defense Department contract to install computer network equipment ... ."

- "concealed fraud by a subcontractor."

- "Boeing repeatedly exported defense articles and defense services to Russia, Ukraine, and Norway without required approval from the Department of State."

- "...settled allegations that Raytheon charged the Government for costs incurred in marketing products to foreign governments."

- "... UTC will pay the US $14.8 million for allegedly conspiring to divert $10 million in US military aid into a slush fund subject to the exclusive control of an Israeli Air Force officer ... ."

- "Pleaded guilty to 37 felony counts of making false certifications to the Department of Defense."

- "wrongdoing associated with foreign military sales of radar systems to Egypt ... ."

These examples were extracted from POGO's (2002) electronic database of cases which specifically under the category of Defense cases:

> …involves military contracts and covers such violations and alleged violations as fraud, cost and labor mischarges, testing falsifications, kickbacks, and bribery. Some of the laws this category covers are the False Claims Act, Truth in Negotiations Act (TINA), Arms Export and Control Act, Foreign Corrupt Practices Act, Racketeer Influence and Corrupt Organizations (RICO), International Traffic in Arms Regulations, and Wrongful Death suits involving military personnel. (POGO, 2002)

The top 43 government contractors, because of their large corporate standings, received over almost half of the contracts awarded, and since 1990, these contractors have paid approximately $3.4 billion in fines, penalties, and settlements. However,

despite the 28 criminal violations and repeat criminal convictions for 4 of the top 10 contractors:

> …only one of the 43 contractors has been suspended or debarred from doing business with the government. This suspension action, against General Electric's Aircraft Division, lasted only five days after they pled guilty to diverting millions of dollars from the U.S. Foreign Military Aid Program to finance the sale of F-16 engines to Israel. (POGO, 2002, p. 1)

These findings indicate a need for maintaining a list or database of contractors and their litigation and criminal history. There is also a need for the imposition of more regular debarment and suspension for contractor misbehavior. This adds an interesting perspective to the outsourcing literature regarding not only procurement practices, but to trust and personnel security practices of the contractors handling major defense, network, and communications systems.

Addressing Elements Leading to Insider Threat Concerns

Many government reports focusing on information assurance specifically mention the insider threat, implying the extensiveness of prospective trend in increased insider threats as a result of increased contracting out of Information Technology. While the government does not realize a central agency or database for tracking insider occurrences it has recognized a growing threat in the form of neglect, misuse, or malicious intent, such as espionage. The insider threat trend is worthy of thorough investigation and monitoring in the DoD to ensure the security of this nation's IT infrastructure and defense-related information systems. For the purposes of this research, a review of information security related reports was established beginning in the late 1980s as the Cold War era was winding down.

Securing Classified Information

In 1985, the DoD Security Review Commission assessed the DoD's efforts in securing classified information. While the primary threat then was still the Soviet Union, and not so much cyber-based as more current threats, the threat of DoD employees and contractors was specifically recognized as a significant problem. In addition to the controlling of classified information, personnel security concerns such as clearances and rules regarding violators were also addressed. At that time stringent policy was in effect for uniformed military, but not for civilian contractor security violators. This report put forth recommendations on ensuring contractors were properly cleared, that clearances were justified using contract numbers, request for proposal (RFP) numbers, re-justified as required, or expired (DoD Security Review Commission, 1985).

Reporting Requirements

Ten years later, the Intelligence Authorization Act for Fiscal Year 1995 required that an annual report to Congress be submitted from the President on the threats to US industry resulting from espionage (Section 809b). This resulted in the National Counterintelligence Center (NACIC) Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. The 1996 update to the NACIC report cited statistics from an American Society for Industrial Security (ASIS) study that "indicated that 74 percent of intellectual or proprietary property losses stemmed from the actions of trusted relationships - employees, former employees, contractors, suppliers, and so forth" (NACIC, 1996, p. 9).

Acknowledging Internet Dependency and Associated Hazards

In 1996 the focus of DoD computer system attacks was a growing threat from external sources, such as hackers. "There is mounting evidence that attacks on Defense computer systems pose a serious threat to national security" (GAO, 1996b, p. 4). The report acknowledged, "that because the U.S. economy, society, and military rely increasingly on a high performance networked information infrastructure, this infrastructure presents a set of attractive strategic targets for opponents who posses information warfare capabilities" (GAO, 1996b, p. 28).

In 1998, the government's increased dependency on computers was further acknowledged as well as a serious deficit in protecting these information resources. The GAO released a report entitled *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, identifying Information Systems as a new high-risk resource (GAO, 1998).

NIPC Stand Up

Also in 1998, the National Infrastructure Protection Center (NIPC) was established as a result of Presidential Decision Directives (PDD) 62 and 63. These PDDs recognized telecommunications systems as a major infrastructure component, as well as the threats now facing this nation as a result of rapid technological development and interconnected systems. NIPC's mission is to "serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures" (NIPC, 1999, p. 7).

Addressing the Cyber Threat from the Inside

In October 1999 NIPC director Michael A. Vatis presented an assessment of the infrastructure threat situation before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism. In this report the insider threat concern is addressed as the "disgruntled insider" being "a principal source of computer crimes," and follows with case examples, including a contractor employee who intentionally deleted U.S. Coast Guard personnel records (NIPC, 1999, p. 5).

Identifying Technology Targets

Information Systems is listed first on the list of "Most Frequently Reported Targeted Technology," in the 2000 NACIC Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. The annual summary of components of espionage-related threats, which includes signal processing technologies explains the threat is not just from foreign governments, but commercial agencies and individuals comprised 26 and 32 percent (respectively) of the information systems targeting (NACIC, 2000).

DoD Examines Insider Threat

In 2000, a report dedicated to the insider threat trend further cemented the DoD's resolve to combat the insider threat. The DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team was a comprehensive summary of shortfalls in lack of data, metrics, and policy in addressing the concern of insider threat activity that exists in the DoD. The agency responsible for the strategy put forth in this document is the Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence OASD/C3I. This report defines an insider as "anyone who is or has

been authorized access to a DoD information system whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector." It specifically addresses "basic sources" of insider threats (maliciousness, disdain of security practices, carelessness, and ignorance pertaining to security policies) (page 6). This document has laid out policy and strategic initiatives to address metrics, data basing, and further research (IPT, 2000).

This report was released in between two insider threat workshops, sponsored by OASD/C3I and Defense Advanced Research Projects Agency (DARPA). These workshops in 1999 and 2000 were dedicated specifically to the insider problem (Anderson et al., 2000).

Security Controls in Contracts

"Six Common Security Weaknesses," outlined by OMB as "government-wide security problems" (OMB, 2001, p.11) were reported in the FY 2001 Report to Congress on Federal Government Information Security Reform. Of note was weakness number five, which addressed security issues specifically in Federal IT contracted functions. Inspector General (IG) reports indicated weaknesses in the DoD's contracting efforts to include "…no security controls in contracts or no verification that contractors fulfill any requirements that may be in place" (OMB, 2001, p. 13).

These reports outlined the threat to DoD systems. They also construed the need for action, metrics, better data, research, and implementation of more stringent operations in dealing with the insider phenomenon confronting DoD IT. Entire organizations, workshops, and policy initiatives are working to identify, estimate, track, and reduce the potential threats to national security by trusted insiders.

However, the reports outlined above only represent the surface of what could potentially be an incomprehensible and immeasurable problem, it is important to recognize the implications of ignoring the information that has been provided. The next section looks at models that have been proposed to study the components of the insider threat.

Insider Threat Models

Of the few studies that have been done on the insider threat, very "few empirical studies of insider attacks are publicly available to guide approaches to this problem" (Schultz, 2002, p. 528). Some very recent literature has emerged that addressed modeling the insider threat from various perspectives. Whether modeling the insider adversary (Wood, 2000) or the prediction of insider attacks (Shultz, 2002; Magklaras and Furnell, 2002), all have recognized the importance of the human factors, with different emphasis on skills, tools, or personality traits.

In a report by Anderson, Bozek, Longstaff, Meitzler, Skroch, and Van Wyk (2000) resulting from one of the aforementioned workshops focused on *Mitigating the Insider Threat to Information Systems*, a basic insider threat model concept was developed. Experts at the August 2000 workshop dedicated to studying the insider threat agreed that although different models will be needed for different situations and environments, there should be a basic framework:

> A comprehensive Insider Threat model would require as a minimum three major components. The components are People, Tools, and Environment. The People component would include parameters such as human performance, behavior, knowledge, and motivation. The Tools component would include all processes, automated or manual; procedures; data; computers; and other devices that people would use to address or solve the Insider Threat problem. The Environment

component would include those parameters that apply collectively to both People and Tools or convey relationships between them. (Anderson et al., 2000)

Anderson and the insider threat research team included in their "confederation of insider models" (2000, p. 23) a macro view model depicting a structure that encompasses functions (undefined at the workshop due to time) to determine predictable behaviors or conditions.

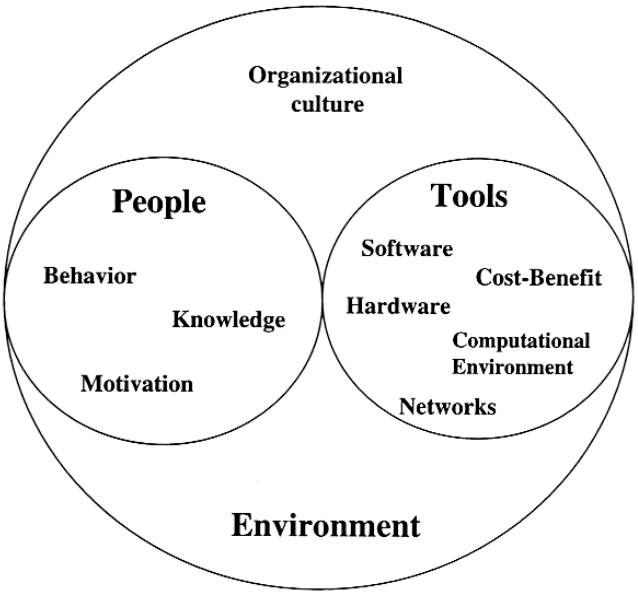


Figure 1: Required Model Components (Anderson et al., 2002)

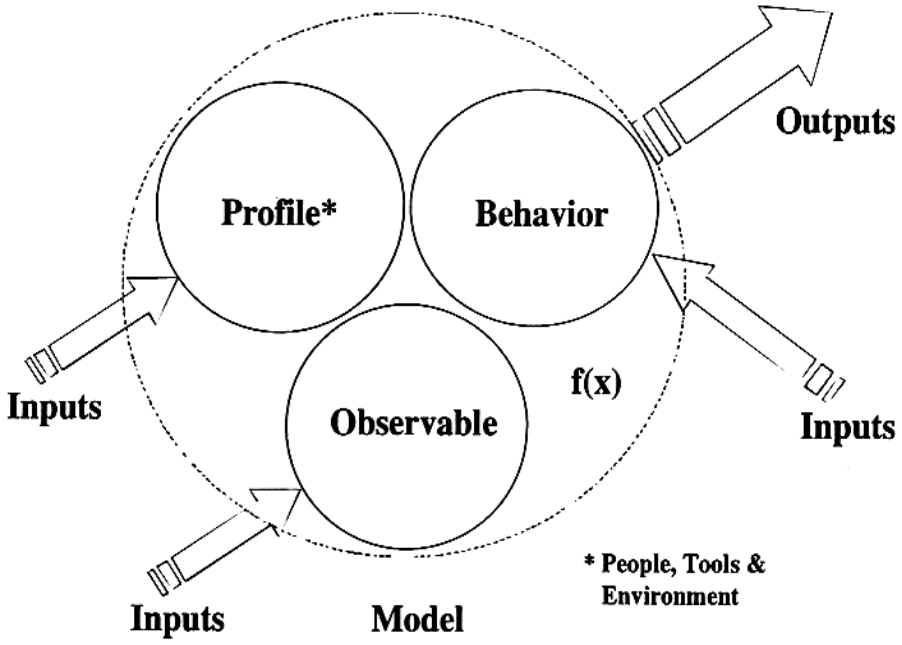


Figure 2: Model Framework (Anderson et al., 2002)

These components will be used as a guide to investigate three other models recently contributed by researchers: B. Wood's *Insider Threat Model for Adversary Simulation* (2000), E. Eugene Schultz's *Framework for Understanding and Predicting Insider Attacks* (2002), and G.B. Magklaras' and S.M. Furnell's *Insider Threat Prediction Tool* (2002).

Attributes of the Insider

Just prior to the insider threat workshop discussed above, Bradley Wood contributed the *Insider Threat Model for Adversary Simulation* (2000) in which he captures the attributes of the malicious insider, which is also included as an attachment to the after action report from this workshop. His model is a simple list of attributes:

"Access, Knowledge, Privileges, Skills, Risk, Tactics (attack behaviors), Motivation, and Process" (2000, p. 1). Each attribute is given certain characteristics that Wood believes simulate actual insider behavior. For example, under the attribute of Motivation, he addresses the expectation that the attacker attempting "force some sort of undesirable consequence within an enterprise to forward one of the following goals: Profit, Provoke change, Subversion, Personal Motive" (Wood, 2000, p. 2).

Magklaras and Furnell give Wood credit for developing "the first comprehensive approach for devising a model that simulates the behaviour of malicious insider" (2002, p. 71). Wood's model is also referenced in Schultz's accounting for his preparatory behavior construct in which attack intentions can be exposed though preliminary activities and the "Use of commands such as ping, nslookup, finger, whois, rwho, and others" (Schultz, 2002, p. 530).

Potential Indictors of Insider Attacks

E. Eugene Schultz's model depicting indicators for predicting insider computer attack consists of: Deliberate markers, Meaningful Errors, Preparatory Behavior, Correlated Usage Patterns, Verbal Behavior, and Personality Traits.

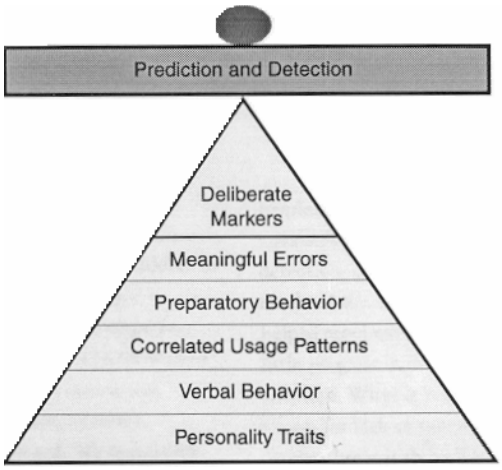


Figure 3: Potential Indicators of Insider Attacks (Schultz, 2002)

His work states that although the insider attack as not the greatest source of computer attacks (due to firewalls put in place to prevent external attacks), it is the most successful type of attack (Shultz, 2002). He also posits that there is no one certain indicator for insider attacks, and there are significant differences in the external versus internal attack methods due to the human and legal elements of dealing with insiders. It is necessary for traditional crime and computer crime approaches to be enhanced beyond generic Capability, Motive, Opportunity (CMO) models and to "reverse engineer" inside attackers through profiling (Schultz, 2002, p. 528).

Insider Threat Prediction Model (ITPM)

Magklaras and Furnell's model is intended to analyze system activity and a user's logged system behavior cues in order to classify users into the following "main insider categories: Possible Intentional Threat, Potential Accidental Threat; Suspicious; and Harmless" (Magklaras and Furnell, 2002, p. 69). Unlike Wood's model, which provides

a list of attributes to help simulate malicious inside attacker behavior, this one considers unintentional misuse by an insider by applying a hierarchy of threat components. They use a mathematical approach to determine values for each attribute and assign quantifiable values and adjustable metrics in order to predict the nature or level of a potential human threat (Magklaras and Furnell, 2002).

(top level) $EPT = \Sigma F_{\text{threat components}} \Rightarrow$

$EPT = F_{attrib} + F_{behavior} + F_{imsinfo} \Rightarrow$

(second level) $EPT = C_{role} + C_{tools} + C_{hardware} + F_{behavior} + F_{imsinfo} \Rightarrow$

(third level) $EPT = C_{role} + C_{data} + C_{hardware} + F_{knowledge} + F_{content} + F_{network} + F_{imsinfo} \Rightarrow$

Figure 4: The Three Layer ITPM Function Hierarchy (Magklaras and Furnell, 2002)

Magklaras and Furnell also reference an Intrusion Monitoring System (IMS) as one of their constants and functions; however, the intrusion "records produced by the Intrusion Monitoring System 'Archiver' module" (2002, p. 73) are part of yet another conceptual architecture that is not specified in this literature. This model seemed to be the most complicated to operationalize, and requires weighted values for each construct (constant). Also, although the authors claim their model is human centric, the table highlighting model constructs shows Schultz's model to lend a more well-rounded account for the human behavior aspect.

Like the other models, this model has yet to be empirically tested.

Model Concept Definitions

Some of the less obvious definitions that reference the People component of the insider model are defined below:

Knowledge – Wood (2000) attributes knowledge to the "both the system and the target" (p.1), which includes capability to call upon applications and commands indicative of the "level of sophistication of the user" (Magklaras and Furnell, 2002, p. 73).

Motivation – A manifestation of many possible emotional needs such as "an expression of power to influence events (satisfy a frustrated sense of self-importance), an outlet for anger, … a means of revenge, or a source of excitement" (Heuer, 2001).

Behavior – Characteristics of computer usage patterns, verbal or written expressions of anger or hostility, particularly before an attack (Schultz, 2002, p. 530).

Tactics – Methods used by attacker, which depend on what he hopes to achieve, whether it be malicious code, disruption in service, system failure or destruction, or theft of information (Wood, 2000, p. 2).

Verbal Behavior – See Behavior.

Preparatory Behavior – Behavior that my indicate intentions to attack systems, such as information gathering prior to a planned attack (Schultz, 2002).

Personality Traits – Shaw, Ruby and Post (1998) outlines characteristics found, through "psychological assessment of programmers, computer scientists, computer graduate students, and systems administrators" (p. 2). These characteristics, in addition to introversion, are "direct implications for risk…including a history of personal and

social frustrations, computer dependency, ethical flexibility, reduced loyalty, a sense of entitlement, and a lack of empathy" (p. 3).

Deliberate Markers – Defined by Schultz (2002) as trademarks, obtrusive or subtle, intended to "make a statement" (p. 530).

Meaningful Errors - Schultz (2002) describes these as mistakes or typos during the attack process that can be found in error logs or other evidence.

Skills – Like knowledge of the system, skills allow the attacker to carry out actions based on their expertise within system domains (Wood, 2000)

Risk – Wood (2000) credits the would-be inside attacker as taking precautionary actions through either working alone or being very furtive in his actions so as to avoid being caught before the attack as been accomplished.

Correlated Usage Patterns – Patterns of usage that can be found on several systems may indicate intended attacks "such as grep on dozens of systems to search for files with particular words in them" (Schultz, 2002, p. 530).

The constructs of all three models are shown in table three as compared to Anderson et al.'s, basic model components. Although some constructs indirectly address components (indicated in the chart by "(X)") in the text of their work, this table uses the original construct names as assigned by the authors. For example, Wood accounts for the major Behavior component under Tactics; Schultz addresses Behavior under basically every construct of his detection model.

Table 3: Insider Threat Model Concepts

Author Model Construct	Anderson et al. (2000)	Wood (2000)	Schultz (2002)	Magklaras and Furnell (2002)
Environment				
Organizational Culture	**X**			
Role (w/in organization)				X
People				
Knowledge	**X**	X		X
Motivation	**X**	X		
Behavior	**X**	(X)	(X)	X
Tactics		X		
Verbal Behavior			X	
Preparatory Behavior			X	
Personality Traits			X	
Deliberate Markers			X	
Meaningful Errors			X	
Skills		X		
Risk		X		
Correlated Usage Patterns			X	
Tools				
Software	**X**			
Hardware	**X**			X
Cost Benefits	**X**			
Networks	**X**			X
Computer Environment	**X**			
Privileges		X		X
Access		X		X
Process	**(X)**	X		
Data	**(X)**			X
Content (user's file entries)	**(X)**			X
Intrusion Monitoring Systems (IMS)/logs	**(X)**			X

Anderson et al. (2002) describe Organizational Culture under the Environment component as the interaction between People and Tools. A formal definition of organizational culture is by Edgar Schein in his book *Organizational Culture and Leadership*:

> The pattern of basic assumptions that a given group has invented, discovered, developed in learning to cope with its problems of external adaptation and internal integration, and that have worked well enough to be considered valid, and therefore to be taught to new members as the correct way to perceive, think, and feel in relation to those problems. (1985, p. 385)

This is relevant concerning outsourcing of IT because it is the Environment and the Organizational Culture that have given the social perspective as to why organizations outsource and the potential affects on workers. Magklaras and Furnell (2002), although having composed a mathematically based model, did, in fact, address all three components under the model requirements put forth by the researchers during the insider threat workshop. They did not name Organizational Culture specifically, but did address the role of the individual as it applies to his place in the organization "with reference to a specific computer system (workstation, server, telecommunication system)…the type and level of system knowledge they possess" (p. 64).

Research Perspective

The insider threat to outsourced information technology is a phenomenon that is not only an observable real-world problem, but it embodies a range of fields of research extending from psychology to economic theory. It is also a research area in which few rigorous studies have been done, due to insufficient discernable case data. Since this is a new area study, with no established formal theory, qualitative research methodologies were consulted.

Qualitative Analysis

Qualitative research is defined as, "any kind of research that produces findings not arrived at by means of statistical procedures or other means of quantification … research about … organizational functioning, social movements or interactional relationships" (Strauss and Corbin, 1990, p. 17). Marshall and Rossman (1989) guide the qualitative process in this case where "research questions explore new territory, previous literature and theory may be inadequate for constructing frameworks for study" (p. 38).

By exploring the insider threat problem from a multidimensional perspective, the results of this study are intended to present a case for future data gathering in order to monitor insider threat trends. By reviewing literature from related fields, a conceptual framework is developed from "theoretical constructs, categories, and their properties that are used to organize the data and discover new connections between theory and real-world phenomena (Marshall and Rossman, 1989, p. 41). An inductive strategy for generating theory, by allowing it to merge from the data that is collected, is explored through grounded theory methodology.

Grounded Theory

Barney Glaser and Anselm Strauss put forth an approach known as grounded theory that is ideal for researching the insider threat to outsourced IT. Grounded theory is often used as a qualitative methodology is ideal for an inductive analysis for a phenomenon for which there is no established, formal theory. While qualitative strategy encompasses theoretical sampling, experiential data, content analysis, literature integration, and historical analysis to achieve conceptual density, grounded theory

specifically strives to "transcend the literature and synthesize it at the same time" (Glaser, 1998, p. 120).

The main thrust of grounded theory is to "Generate Theory that accounts for a pattern of behavior which is relevant and problematic for those involved" (Glaser, 1992, p. 75; Straus, 1987, p. 34). The theoretical framework that developed through grounded theory begins with categories and properties, as defined in the following set of definitions from the varied works of Glaser and Strauss:

Category – "Stands by itself as a conceptual element of a theory" (Glaser and Strauss, 1967, p. 36). "A classification of concepts" (Strauss and Corbin, 1990, p. 61).

Property – "Conceptual aspect or element of a category" (Glaser and Strauss, 1967, p. 36). "The most concrete feature of something (idea, thing, person, event, activity, relation) that can be conceptualized, which will allow the order of specificity required by the analyst for purposes of his or her research" (Strauss, 1987, p. 21). "Attributes or characteristics pertaining to a category" (Strauss and Corbin, 1990, p. 61)

Conceptual Density – "The multiplicity of categories and properties and their relationships" (Strauss, 1987, p. 21).

Hypothesis – Generalized relationships among categories created by comparing similarities and differences among groups (Glaser and Strauss, 1967). "A provisional answer to a question about a conceptual relationship" (Strauss, 1987, p. 21).

Core Category – "The central phenomenon around which all the other categories are integrated" (Strauss and Corbin, 1990, p. 116).

These concepts typically emerge from reviewing large amounts of literature and data that is related to the field of study, when no relevant literature base for the primary

area of study (in this case, insider threat to outsourced information systems) is available. By taking notes on the data that are then sorted into categories, one can then extract properties to determine the conceptual density of the research problem.

Forced and Emergent Philosophies

From the co-founders of grounded theory, Dr. Barney Glaser and Dr Anselm Strauss came two seemingly polar philosophies of doing grounded theory, although their original work *The Discovery of Grounded Theory* (1967) was a cooperative effort. While the main goal of both methodologies was to generate theory, Strauss takes on a more structured approach to categorizing and coding the data. It is believed this procedural approach was to help the research assign scientific rigor to qualitative research methodologies. Strauss (1990) also classifies grounded theory as a qualitative, inductive research method; Glaser shows it to be a quantitative or qualitative approach, but still inductive in nature, conducive to academic freedom for the independent researcher (1998).

Glaser's emergent philosophy insists that pure grounded theory is not "forced" through rigid classifications, common with other methodologies. Although still rigorous, grounded theory, according to Glaser, allows the researcher to be guided by the data, and not the other way around (1998).

Summary

This section reviewed the literature pertaining to documented insider threat information, proposed models for studying the threat, and perceived trends. Outsourcing

theory literature was also reviewed, as it applied to outsourcing information technology and the trends toward this movement.

The human aspect of the threat, the insider, was reviewed via the results of psychological and sociological professionals specifically focused on insiders, spies, and computer criminals. A larger sociological and economic picture was also presented with respect to the culture that has been promulgated by information technology, outsourcing trends, the global workplace, and information distribution and access. Employee loyalty and ethical flexibility from an individual psychological perspective and a social perspective was also reviewed in terms of contracted employment and foreign influence.

An historical analysis if the government and DoD's multidimensional efforts to address the security and technological issues related to insider activity, malicious or otherwise, was presented as a basis for understanding applicability of this research in a national security role.

Finally, an examination of the literature on qualitative research methods and grounded theory were reviewed, as these references were the genesis for the alternative research methodology used in this study.

The next chapter presents the methodology used in analyzing available literature, reports, studies, and cases.

III. Methodology

> "DoD's strength is our use of information technology; our weakness is our use of information technology." (Money, 1999)

Introduction

The previous chapters gave an overview of outsourcing theory, psychological and social concerns, and security considerations regarding information technology and the threat of the insider. This chapter explains the methodology used in determining whether there is a significant relationship between the insider threat and the growing trend of outsourcing IT.

Research Goals

The primary goal of this research was to determine whether government information technology has become more vulnerable to threats from the insider in light of contracting information systems operations and maintenance to outside agencies.

The term insider threat has been used on an increasing basis in government testimony by organizations such as the FBI, NIPC, and OSD/C3I. Task teams and workshops have been dedicated to examining the potential threat of the insider. The focus of this research was to determine whether the popularity of outsourcing government information technology is a contributing factor to the insider threat.

The motivation for this research was originally the observation of blue suit operations that have been contracted out during the last decade of the 20th century. The

drawbacks of outsourcing have been discussed in literature, such as marked reduction in quality of service and reduced flexibility (Lacity et al., 1995; Grover et al., 1996; Antonucci et al., 1998; Klepper and Jones, 1998; Tayntor, 2001). The security aspect has only been mildly addressed (Fink, 1994) and often, "Unfortunately, risk assessment takes a backseat before, during, and after negotiating an agreement" (Kliem 1999, p. 93). In the case of government information technology where missions of national defense are concerned, it is believed that the threat posed by the insider has been severely underestimated (OMB, 2001). There is no established process in place or central database available to manage these cases, as addressed by the DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team (2000).

Abused or misused system access by the disgruntled or otherwise ill-meaning insider has become a purportedly more common occurrence, however, the data to support this has been elusive at best. While the literature review addresses the DoD's increased interest in the insider threat since the late 1980's, there are apparent significant shortfalls in the monitoring and evaluation of security incidents in the contracted information systems.

Assumptions

1. Information obtained on information technology that has been contracted is representative of general government outsourcing of similar systems, unless documented otherwise.
2. Studying the entire DoD outsourcing situation is beyond the scope of this research (or availability of data is restrictive in nature).
3. This research is restricted to information technology that has been outsourced which includes, but may not be limited to, telephone switches, network

control centers, intelligence data systems, communications centers, or communications maintenance activities.

4. Data has been severely limited or restricted at best. This in itself is may be a possible indication that information on security violations from the inside should be more closely tracked.

5. Available data may be skewed due to the amount of incidents not reported to investigative agencies and are handled within the organization.

Data Availability

This is a relatively new area of advanced study, therefore, information collection was from a variety of sources. An extensive search effort for data included several DoD agencies which took an interest in this topic and had initially offered to contribute their limited case data as applicable to this study. However, currently, no central source of statistical case data exists. According to Anderson et al., (2000):

> Little data exists today specific to the Insider Threat. What data exists is spread throughout many organizations and usually has distribution limitations preventing its use throughout the research community. Furthermore, the depth and breadth of such data is inconsistent. Reference control data is needed for evaluation research, progress, and results. Such data is essential to developing and validating Insider Threat models. (p. 25)

Desired data collected was originally to be based on the following:

- Number/proportion of outsourced IT functions in the Air Force (telephone switches, network activities) between 1990 and 2002 (MAJCOM sources)
- Date/time period of internal security incident occurrence
- Outsourcing status of function in question (government, outsourced, or pending outsourcing)
- Nature of occurrence (neglect, misuse, or malicious intent, such as espionage, corporate, industrial, or otherwise)
- Personnel involved (military, civilian, contractor personnel)

Analysis methods would depend on the data collected, but optimally would involve regression methods to determine the most statistically significant cause, if any, to a rise in insider threat activity.

Desired preliminary prediction variables were:

- Proportion of outsourced IT functions AF-wide;
- Whether incident was action of contractor, civil servant, or uniformed military personnel;
- Whether the activity one of the following:
    - blatant malice (including espionage and any intent to harm national security),
    - neglect or abuse (includes disregard for policy and security regulations),
    - or misuse (using the systems for other than original intent for personal gain, however, without intention to harm the government),
    - Other factors applicable to analysis

Investigative agencies and information operations centers were contacted for case data demonstrating security incidents from the inside. Requests were made for data on the base location, nature of incident, and whether the incident was committed by military, civilian employee, or contractor, as well as impact (financial or otherwise) on the unit.

In addition to investigative agencies, stateside major commands and contracting sources were contacted for information to determine which bases had outsourced telephone switches (operations and maintenance) and network control centers. A database was to be constructed to depict the amount of outsourced functions. It was found that few commands do not outsource their network control centers (NCCs) because IT is considered to be a core competency (an inherently governmental function of the organization's mission). The one definitive discovery was that more than half the stateside telephone switches at major installations (38 out of 62) were outsourced. In

addition, dates reflecting when communications functions were outsourced were unavailable for retrieval as major command agencies did not monitor outsourcing dates and other data on their bases, and some chose not to release what data they had.

During the search for data to support this research, it was also found that there are no metrics, central databases, or releasable case files for identifying which security incidents were committed by insiders. The Insider Threat IPT of April 2000 has already identified this shortfall.

A very limited number of releasable cases of insider intrusions reported to investigative agencies were found. Managers of operations and maintenance contracts also had no security incident records for contractor personnel operating and maintaining telephone switches. Defense Personnel Security Research Center (PERSEREC) in Monterey, California has done some research in this area as well, using the limited closed case files from the military investigative agencies, although not specifically relating to the outsourcing questions.

Without the data originally required for a statistical evaluation of the outsourced information technology situation across a stateside sampling of Air Force bases, the quantitative methodology originally proposed was determined to be inappropriate to continue research in this area. However, the information gained from the literature review indicates this is still a valid and much needed research endeavor. Therefore, the absence of numerical data forced the research effort to state a revised focus question:

If there is little reliable, detailed data, how is it the threat of the insider is thought to be increasing?

Qualitative Strategy Formation

With the lack of data to support this research, it was important to ensure the review of the information available on this topic was scrupulously studied to try to determine the impact outsourcing information technology has had on the insider threat trend that is reportedly on the rise.

A qualitative approach was decided upon based on this research question requiring "the exploration of a process not yet identified and not yet encompassed in theory" (Marshall and Rossman, 1987, p. 36). Although a qualitative analysis methodology originally served as an alternative for insufficient statistical data sources, it appears to be the most appropriate approach for this topic. By using methods set forth in grounded theory, related research categories emerged from the literature and are presented for analysis in Chapter Four. Academic literature on outsourcing theory, psychological typing of IT professionals, as well as sociological aspects of the global business environment, including foreign influence and anti-American sentiment was consulted. Literature on employee loyalty and psychological contracts was also reviewed. Furthermore, the systemic domain of personnel security and screening procedures and monitoring of contractors and procurement practices that have caused financial damage to the federal government added to the subsequent concept that all these elements are interrelated and present when outsourcing IT.

This inductive review intends to not only indicate a variety of attributes of outsourcing and information technology, but to demonstrate how the interrelated elements fully comprise observable patterns of increased insider threat. By

understanding how the combination of these individual components threatens the information processed and managed, it may be possible to address the threat, and propose an integrated model to support a theory that will provide a case for future data gathering (Marshall and Rossman, 1989) and testing.

Modeling Outsourced Information Technology

The basis for a proposed model is the interconnecting of the following areas of study: outsourcing theory, psychological, socio-economic, and systemic. Under the outsourcing theory purview, traditional economic and strategic management-based approaches to outsourcing have been applied by managers since the early part of the 20th century. These approaches are based predominantly on the costs, assets, tasks, personnel skills – primarily resources – and the benefits an organization can reap while striving toward their goals. However, these approaches to outsourcing were antecedent to the modern interconnected and global environment; outsourcing is often addressed as a function of economics first and foremost, with security risks often an afterthought. Outsourcing is a business practice now commonly applied to the DoD, including information technology operations and maintenance (telephone switches and network control centers), which are not considered by some agencies to be core functions. "In addition, DoD has conducted the largest competitive sourcing program in the federal government, and is planning to compete 15 percent of those positions not deemed inherently governmental by 2003. Competitions are spread out over a wide array of military base functions, including communications, computing, and maintenance and repair" (OMB, 2002, p. 5).

Building on the outsourcing practices applied to information technology, there are socio-economic and psychological factors that apply to the insider threat vulnerability. The psychological aspect of the typical IT professional, as defined by employment status and length, in addition to observed personality traits is a contributing factor to the suspect employee loyalty as a result of a contracted employment situation in a modern, interconnected, highly-technical information environment.

Paralleling the employee loyalty aspect of the temporary employment of the IT professional is the foreign influence. The contracting of sensitive, classified, software and information technology to companies owned by foreign countries, coupled with increased anti-American sentiment globally, adds an aspect of risk from the inside that could be potentially devastating to information systems. The employee loyalty factor is primarily examined under the sociological domain for the purpose of this research, however, it has strong connectivity to the psychological perspective where typing of the IT professional is concerned.

Finally, the systemic category observes characteristics of the DoD in which the environment possibly fosters the presence of the threat. The current backlog of personnel security clearances and failing of supporting databases are relevant to this research, as this shows a significant vulnerability in the clearance process for contractor personnel.

An important part of this research was the completion of a thorough historical analysis of the DoD's efforts to identify and counter the suspected threats posed by the ill-meaning insider. Reports presented here add a temporal and historical relevance to the evolution of the insider threat concern.

Grounded Theory Methodology

The topic "insider threat," as it applies to information technology and outsourcing, is a relatively underdeveloped classification of study in academic literature. As this research has shown, there is very little data to accommodate whether the insider threat is a growing problem. However, there is a strong belief that this threat is real, growing, and should be a national security concern. This belief is grounded in the study of aforementioned categories that appear to be interrelated.

Qualitative strategies, grounded theory in particular, were called upon due to the complex social relationships forming in this research area. This methodology provides grounds for future data collection (Strauss, 1987) that may be generalizable to the entire DoD IT outsourcing process. By demonstrating the interrelationships and overarching properties of sampled research domains (categories), conceptual density is achieved from which a theory can be generated.

Chapter Four will give an in-depth analysis of the theoretical connections between the following categories and their substantive properties. The analysis will show that in this particular application of qualitative research, the data that was gathered is used to develop a theory as opposed to testing it (Glaser, 1998).

The data were analyzed using a form of open coding methodology to identify categories and properties that classified the research areas. A form of axial coding was considered to make "connections between a category and its subcategories" (Strauss and Corbin, 1990, p. 97). Finally, selective coding techniques describe the relation of the core category (insider human threat) "to the other categories, validating those relationships" (Strauss and Corbin, 1990, p. 116).

Weaknesses

This methodology's primary drawback is in the data is that no statistical data was available for this analysis. While investigative sources are concerned about the insider threat, their limited case data did not reflect what they believed was the true magnitude of the problem.

Another limitation was some significant contention in the grounded theory literature between the founders (Anselm Strauss and Bernard Glaser). Sources by both authors were used and the result was a combination of their methodologies. The emergent philosophies of Glaser are evident in the reformation of the research question as more categories emerged from the literature review process. The structured approach of Strauss was used in leveraging the four main categories to form a conceptual model. Therefore, the inductive, qualitative analysis developed in this work may be considered a merging of emergent and forced philosophies.

Surveys

Surveys are tools that may be used by social scientists to measure perceptions on the insider threat. However, "are of little value for examining complex social relationships or intricate patterns of interaction" (Marshall and Rossman, 1989, p. 85). It was determined this was not the best approach for this particular topic. This is a controversial topic of discussion among communications professionals; the communications community has essentially been bombarded by surveys from other AFIT and organizational endeavors. Furthermore, the complex social relationships explored in this research require much more time, permission, and sensitivity than the scope allowed.

Summary

This chapter reviewed the methodology used in determining relationships between categories of literature and information relevant to investigating the insider threat to outsourcing and information technology.

The next chapter gives an analysis of the information and presents the cross-connected categories and properties. A model is then constructed operationalizing the relationships and constructs generated by the analysis.

IV. Analysis

Introduction

This chapter investigates the more complex research problem generated in Chapter Three: *If there is little reliable, detailed data, how is it the threat of the insider is thought to be increasing?* By exploring the data related to outsourcing, insider threats, and information technology (literature, cases, articles, testimonies, and reports) a framework is constructed that shows the logical connections behind this statement.

Research Elements

The concept of the insider threat is composed of several components. First, there is the outsourcing theory aspect. In attempting to develop an outsourcing philosophy for the federal government, economic goals and strategic management issues regarding manpower prevailed. It was believed that money could be saved and highly technical skill-sets could be acquired by seeking help from outside organizations. However, by studying models put forth by economic and strategic management theorists with regard to information technology, one observes the models do not address modern concerns of risk analysis to include the fiscal and operational aspects of accounting for and recovering from threats posed by an unreliable employee.

While the outsourcing theory aspect of the insider threat model could most likely be modified to consider the risks posed by making an outsider an insider, the next aspects are psychological and social considerations, some unique to the highly technical fields.

These psychological and socio-economic aspects address personality traits observed to spawn behavior in computer professionals that could be malicious in nature and potentially damaging to an organization. The socioeconomic perspective investigates perceived increases in the global business environment, anti-American sentiment and foreign influence, and contracting to foreign-owned companies. These factors are hypothesized to be contributors to decreased employee loyalty.

In addition to the theoretical and psychological and social aspects of the insider threat apparently plaguing information technology, systemic causes, brought about by several factors also have an impact. Military downsizing and trends toward contracting out skills that are not seen as inherently governmental add a mentionable burden of obtaining security clearances for personnel accessing government facilities and systems. The reduced manning in the defense investigative services is now bearing the burden of investigating those contractor personnel not formerly possessing clearances. Given that contractors are often responsible for ensuring their subcontractors meet qualifications set forth in contracts, the government or hiring agency has no guarantee subcontractors are adequately cleared. Finally, there is an intense backlog in security clearance process for the people already cleared and undergoing revalidation. In the systemic realm, we account for inadequate regard for existing security policy, and inefficient monitoring and tracking of incidents resulting from the insider.

Enabler of Vulnerabilities

Although not implying that outsourcing is inherently corrupt, the initial analysis examines outsourcing theory as an enabler of conditions having a potential for fostering

vulnerabilities. These vulnerabilities are created by factors such as existing conditions, interactions among actors, strategies and tactics, and consequences (Strauss, 1987) that are characteristic of each outsourcing theory's basic philosophy. These contributing factors were then cross-connected with properties of the other major constructs to show interrelationships to the insider threat situation which is assumed to increase with respect to scope, severity, and time. Willcocks and Lacity (1995) summarize these conditions and factors in their statement:

> IS outsourcing is different from outsourcing anything else…on five counts:
>
> (1) IT evolves rapidly; this surrounds IT sourcing decisions with a high degree of uncertainty.
>
> (2) The underlying economics of IT changes rapidly. Although for example price/performance improvements occur in every industry, in few industries do the underlying economics shift as fast as in IT.
>
> (3) The penetration of IT to all business functions is becoming ubiquitous: unlike many other products and services IT cannot be easily isolated from other organizational functions.
>
> (4) The switching costs to alternative information technologies and IT suppliers are high, and sometimes prohibitive.
>
> (5) Many potential and actual customers are still highly inexperienced in IT outsourcing. This can put them at a significant disadvantage when negotiating and running contracts with outsourcing vendors. (p. 206)

This model also accounts for psychological and social impacts on people and organizations as rapid technology proliferation further permeates many aspects and dimensions of society. I found it interesting that the first and second counts relate to existing conditions of rapid technological change or information technological trends and economic trends.

The third count deals with IT and organizational culture, stressing the interaction factor, as IT is deeply ingrained in all facets of business and modern society. Strategies are played out in the fourth count listed above when management must make decisions based on transaction costs, agency costs, resource gaps, and information technology trends. Finally, consequences of economic and strategic management decisions (to outsource some, all, or none of the organization's IT) can also reflect in organizational culture, uncertainty, increased (or decreased) costs, and risks – all properties of the category of outsourcing theory.

The theoretical approaches to outsourcing, as well as the psychological, socio-economic, and systemic or organizational aspects of the overall insider threat are interrelated and overlapping, which makes the problem a multi-faceted threat to our information systems, and ultimately, our national security. These interrelationships are found between the categories and properties addressed by the next section.

Generation of Theory

The theory generated here was developed through progressive levels of perspective, as prescribed by Dr. Barney Glaser in his grounded theory literature. The first level is the data itself, from which emerged the categories. The essential elements of each category were then analyzed for properties describing the event or instance stated or taking place in the data, which forms the second perspective level.

At the third perspective level, termed substantive theoretical level by Dr. Glaser, integration takes place as the categories and properties are "sorted into theory" (1998, p. 136). The model produced by this methodology bears the relationships between the

substantive theoretical codes (categories and properties). The theory can then be tested through applied cases and events (Glaser, 1998).

Categories of Data

As mentioned previously, the categories emerged during analysis of the information (all of which is considered data), literature, reports, and proceedings relevant to the research area of insider threat in the outsourced information technology environment. Each category contained properties that were determined by patterns of behavior (in case studies), incidents or occurrences that were interrelated between categories.

By discovering interconnections between these knowledge bases, relationships were found that give a multidimensional perspective to what is more than just computer crime. As the information was analyzed, and more was gathered, it was found the insider threat research area to be an emergent culture in itself as a result of years of actions on the parts of scientists, economists, managers, and social scientists. Each category presented here, along with its associated properties, impacts properties and other research areas to feed into a cycle of a phenomenon that is believed to be growing in complexity and scope over time.

The ideas presented in the following sections represent the individual categories and their revealed properties. The properties were then cross-connected to each other in an attempt to see whether or not conceptual density was present in the data. If it can be shown that the relationships between these categories are theoretically dense (by showing definite interconnectivity among multiple properties), then the proposed model would be

relevant, working, fitting, and modifiable (Glaser, 1992) in basic grounded theory form. This model could then serve as a multidimensional theoretical demonstration of the insider threat phenomenon. Implications for use of this model will follow in Chapter Five.

The conceptual framework encompasses an explanatory network of forces impacting the scope, severity, and complexity over time, and magnified by the events posited in each category. The forces all interconnect to shape and add dimension to the insider threat facing our critical information systems and infrastructures.

Category Analysis

The elements of each category of reviewed literature were extracted as elements that are believed to be contributing factors to the properties composing the each construct of the final model.

Glaser (1998) gives guidance for extracting properties by asking the following questions (p. 140):

1. What category is indicated?
2. What property of what category does this incident indicate?
3. What is the main concern of the participants?

The categories themselves emerged in the initial search for literature pertaining to the insider threat. From these categories emerged properties that were used to connect the categories as model constructs.

The next four sections gives second-level perspectives of the categories by displaying properties believed to best describe each incident. Most incidents were pulled

verbatim from sources cited, to ensure proper context of the author was understood. The elements from the literature were indicative of the more popular theories used to speculate on outsourcing IT for the scope of this research. It was found that costs and contractual issues addressed material or resource based business concerns in outsourcing more than the behavioral or social issues, such as organizational culture and trust concerns with opportunistic behavior. This is to be expected. Most outsourcing literature pertaining to IT is based on economic and strategic management theories and not social theories.

Outsourcing Theory and Principles

The first category in this analysis examines the theoretical perspectives of outsourcing IT and principles laid out in peer-reviewed literature. This aspect is appurtenant due to the conditions that call for a management decision to outsource or the resulting conditions brought about by outsourcing. This decision is brought primarily about by cost and resource factors that have been studied heavily in Economic and Strategic Management Theory.

Table 4: Outsourcing Theory Second Level Perspective

Theory of IT Outsourcing	Properties
Determines most efficient contract (behavior oriented – delegates some decision-making authority to the contractor) (Cheon et al., 1995)	Contract Complexity/Length Agency Costs
Uncertainty due to government policies, economic climate, technological change influence agency costs (Cheon et al., 1995)	Agency Costs, Uncertainty, Technological Trends, Economic Trends
Uncertainty due to environmental dynamics and rapid technological change forces firms to focus on core competencies (Slaughter and Ang, 1996)	Uncertainty, Core Competencies, Technological Trends
Risk aversion of outsourcing receiver or provider influences agency costs (Cheon et al., 1995)	Risk, Agency Costs
Programmability determines specified appropriate behavior by vendor influences agency costs (Cheon et al., 1995)	Agency Costs, Contract Complexity/Length, Measured Outcomes
Extent to which outcomes can be easily measured influences agency costs (Cheon et al., 1995)	Measured Outcomes, Agency Costs, Contract Complexity/Length
Length of agency relationship (contract) influences agency costs (Cheon et al., 1995)	Agency Costs, Contract Complexity/Length
Primary reference point for outsourcing research literature (Clark et al., 1995) Transactions (exchange of goods/services) are evaluated for economic efficiency (Cheon et al., 1995)	Economic Trends, Transaction Costs
Uniqueness/specificity of hardware, software, and skills increase transactional relationship with contractor (Cheon et al., 1995)	Core Competencies, Transaction Costs
Uncertainty conditions (unpredictable market, technological, economic trends, contractual complexity, quality of outputs) increase transaction costs (Cheon et al., 1995)	Uncertainty, IT Culture, Economic Trends, Transaction Costs, Contract Complexity/Length
Infrequency of contracting due to initial building of relationships with new contractors increase transaction costs (Cheon et al., 1995)	Transaction Costs, Contract Complexity/Length
Implies more likely (and natural) opportunistic behavior on the part of the vendor, thus increasing transaction costs (monitoring behavior) (Clark et al., 1995; Jurison, 1995)	Opportunistic Behavior, Transaction Costs
Outsourcing is done to fill gaps in information systems resources and capabilities (Cheon et al., 1995)	Resource Gaps

Information systems capabilities include information quality, staff, support, cost effectiveness) (Cheon et al., 1995)	Resource Gaps
Resource attributes include value to the firm, uniqueness to the firm, non-substitutable by competing firms, and not imitable by other firms (Cheon et al., 1995); these attributes provide competitive advantage (Mata and Fuerst, 1995)	Core Competencies, Resource Gaps
All organizations depend on resources from other organizations for survival (Cheon et al., 1995)	Resource Gaps, Resource Dependency
Relationships in task environments (concentration, availability of scarce resources, and interconnectedness) impact resource dependent outsourcing strategy (Cheon et al., 1995)	Resource Gaps, Resource Dependency
Resource dimensions (importance, discretion over use, and control over resource) impact resource dependent outsourcing strategy (Cheon et al., 1995)	Resource Dependency, Resource Gaps
General Resource Theory – Intangible resources are information based; technological innovation and culture are resources. (Claver et al., 1998; Mata and Fuerst, 1995)	IT Culture, Organizational Culture
General Resource Theory – Technological innovation can be considered a competitive resource if it has large R&D department, infrastructure, and strong corporate culture. (Claver et al., 1998).	IT Culture, Core Competencies, Organizational Culture
Outsourcing relationships with high uncertainty, high risk aversion, low programmability, low outcome measures, and longer relationships have highest agency costs (Cheon et al., 1995)	Uncertainty, Risk, Contract Complexity/Length, Agency Costs, Measured Outcomes
Keeping technology up to date, emerging technology (Antonucci et al., 1998; Grover and Ramanlal, 1999 Tayntor, 2001)	Technological Trends, IT Culture, Resource Gaps, Transaction Costs
Costs and benefits of worker employment environment (Slaughter and Ang, 1996)	Organizational Culture, Agency Costs, Employment Conditions/Relationships
Competition and Cost Savings (Antonucci et al, 1998)	Economic Trends, Resource Dependency
Access to variety of new resources, skills, technology (Lacity and Hirschheim, 1994; Antonucci et al., 1998; Jurison, 1995; Slaughter and Ang, 1996)	Technological Trends, IT Culture, Resource Gaps
Internal IT departments viewed by some managers as archaic, expensive, unmanageable (Antonucci et al, 1998)	Technological Trends, IT Culture, Transaction Costs
Loss of control, flexibility concerns (Antonucci et al., 1998; Tayntor, 2001)	Risk, Disaster Recovery, Contract Complexity, Measured Outcomes, Agency Costs, Uncertainty

Vendor use of subcontractors (Antonucci et al., 1998)	Risk, Contract Complexity/Length Measured Outcomes, Agency Costs
Displacement of employees, layoffs (Antonucci et al., 1998)	Employment Conditions/Relationships, Organizational Culture
Impact of outsourcing on IT security and control (Fink, 1994)	Risk, Agency Costs, Disaster Recovery, Contract Complexity/Length, Measured Outcomes, Transaction Costs
Risk management must be practiced when negotiating outsourcing agreement (Kliem, 1999)	Risk, Disaster Recovery, Contract Complexity/Length, Measured Outcomes, Transaction Costs, Agency Costs
Assumes humans cannot achieve complete contracts, due to inability "to forsee complexities and contingencies in contractual relationships" (Jurison, 1995)	Contract Complexity/Length, Transaction Costs, Uncertainty, Risk
Assumes "decision makers are rational people who adopt organizational forms that best economize on transaction costs" (Jurison, 1995)	Transaction Costs, Risk
Cost benefits are easier to determine (vendor proposals) than risk (many components and dimensions) (Jurison, 1995)	Transaction Costs, Risk
Dynamics of IT skills market (shortage skills, rapid technological change) (Levina, 1999)	Resource Gaps, Technological Trends, Economic Trends, IT Culture

An interesting observation was made here due to speculated strong social and psychological emphasis on the insider threat core category. The vulnerability enabler of outsourcing theory addressed by a hypothesis: *Applications of traditional outsourcing theory to IT inject uncertainty into the organizational environment and downplay human factors indicative of technological culture, thus increasing potential for insider threat.* The "hard" line of business (profit) is often the first consideration when it comes to

outsourcing, therefore counterbalancing security, and increasing potential for adverse insider behavior. The effects of information technology and global society on the organizational cultural, social, relationship, and behavioral aspects of outsourcing transactions are deserving of more significant study in order to reduce potentially vulnerable IT to the insider threat.

The category properties of IT Outsourcing Theory are summarized below:

Table 5: Outsourcing Theory Properties

Outsourcing Theory
Transaction Costs
Agency Costs
Contract Complexity /Length
Risk
IT Culture
Resource Gaps
Measured Outcomes
Technological Trends
Economic Trends
Uncertainty
Resource Dependency
Core Competencies
Disaster Recovery
Organizational Culture
Employment Conditions/Relationships
Opportunistic Behavior

Psychological Impact of Outsourcing Information Technology

"The new information and communication technologies are generating not merely new patterns of work but also new methods of deviancy in the electronic work environment" (Zaiton, 2000, p. 111).

This section examines the psychological perspectives as they relate to the information technology environment as outsourcing becomes more prevalent. It is becoming evident that information technology is not just a function or service, whether or not it is considered an organization's core competency, to be added to a list of chores to be contracted out, such as trash removal or grounds maintenance. Information technology, as stated earlier, impacts many dimensions of our society, an organization's culture, and the minds and motivations of those people who work there. Unfortunately, it is often not easy to evaluate all the risks when considering the impact of maintaining an edge in comes managing our electronic information.

Personality traits and loyalty, along with general indicators of our highly technical culture, dominated the insider threat and psychological contract literature. Opportunistic behavior, although a major tenet of agency cost theory (which could explain its lack of recurrence in other theoretical elements) also occurred in many of the psychological elements. The next table shows second-level perspective of psychological data gathered on this category.

Table 6: Second Level Perspective of Psychological Category and Properties

Psychological Elements of Insider Threat	Properties
Preconditions for insider betrayal influenced by changes in social and economic conditions in US and relations w/ rest of the world (Heuer, 2001) Increased Opportunity	Social Trends, Economic Trends, Internationalization
Preconditions for insider crime: opportunity, motive, character weaknesses, triggers (Heuer, 2001)	Opportunity, Motive, Ethical Flexibility, Triggers, Personality Traits
Presence of a subgroup of computer professionals and computer science students whose entry into computer field was motivated, in part, by frustrations getting along with others (Shaw et al., 1998)	Interpersonal Social Frustrations, Personality Traits, IT Culture
Insider betrayal may be expression of power, influence, revenge; motivation includes emotional needs and not always money. (Heuer, 2001)	Emotional Needs, Power, Revenge, Personality Traits
Loyalty adversely affected by economic changes devaluing long-term employee-employer relationship (Heuer, 2001)	Loyalty, Economic Trends, Employment Conditions/Relationships
Illegal behavior often rationalized by feelings of entitlement to better treatment from employer. (Heuer, 2001)	Entitlement, Employment Conditions/Relationships, Personality Traits
Cases reveal complex issues of loyalty in an international environment (Shaw et al., 1998)	Loyalty, Internationalization, Ethical Flexibility
Dynamic interaction between vulnerable information technology professional (w/ personality characteristics of introversion, etc.) and organization and personal environment causes potential trigger of dangerous insider behavior. (Shaw et al., 1998)	Personality Traits, Employment Conditions/Relationships, Triggers
Personality and cultural characteristics of destructive insider behavior: Introversion, computer dependency, history or personal/social frustrations (anger toward authority), ethical flexibility, mixed sense of loyalty, entitlement, lack of empathy. (Shaw et al., 1998)	Personality Traits, Interpersonal Social Frustrations, Ethical Flexibility, Loyalty, Computer Dependency
Introversion is characteristic of computer technology specialists, scientists, and other technology specialists. (Shaw et al., 1998)	Personality Traits, IT Culture
Introversion found to be common trait in every psychological assessment of programmers, computer scientists, computer science graduate students, and system administrators (Shaw et al., 1999)	Personality Traits, IT Culture

Subgroups of studied computer users include "computer addicted" individuals, prone to share histories of social failures and ostracization; computers replace direct interpersonal relationships; "more likely to be independent, self-motivated, aggressive loners, make poor team players, and feel entitled to be a law unto themselves" (Shaw et al., 1998)	Personality Traits, IT Culture, Interpersonal Social Frustrations, Computer Dependency
Surveyed computer professionals revealed tendency toward looser ethical boundaries within the "information culture" (if a system is not secure, it is game for attack) (Shaw et al., 1998)	Personality Traits, IT Culture
Reduced loyalty found among programmers and other professionals with high demand for services and high rates of turnover. Those identifying more with profession than organization prone to more intellectual property conflicts involving source code, programs. (Shaw et al., 1998)	Loyalty, Personality Traits, IT Culture, Opportunistic Behavior
Current shortage of information technology personnel may influence narcissism among older employees who may resent special treatment and/or bonuses paid to new hires. (Shaw et al., 1998)	Loyalty, Personality Traits, IT Culture, Opportunistic Behavior
Narcissistic personality (sense of entitlement) and anger at authority common among perpetrators from energy and national security infrastructures. (Shaw et al., 1998)	Loyalty, Personality Traits, IT Culture
Organizational commitment pertains to degree of identification w/ organization and its goals. (Millward and Brewerton, 1999)	Loyalty, Personality Traits, IT Culture
An emotionally-detached and self-interested employee who fails to become integrated into the organization is one whose commitments and energies are likely to be focused elsewhere. (Millward and Brewerton, 1999)	Loyalty, Personality Traits, IT Culture, Employment Conditions/Relationships
Lesser degree of loyalty is anticipated from contractors, partners, consultants, and temps due to short term or transient nature of employment (Shaw et al., 1998)	Loyalty, Employment Conditions/Relationships, Length of Employment, Opportunistic Behavior
Study by Millward and Brewerton (1999. p. 266): Found that "contractors (both permanently and temporarily employed by the agency) were more likely than employees to be transactional in orientation and to hold a short term view of their future with the client company"	Loyalty, Employment Conditions/Relationships, Length of Employment, Opportunistic Behavior, Transaction Costs
Transactional psychological contracts based on pay for short term employment (Millward and Brewerton, 1999) (Economic based)	Employment Conditions/Relationships, Length of Employment, Opportunistic Behavior, Transaction Costs

Findings of 1999 study show it is possible for contractors to be integrated in the workplace on a partnership basis so long as outsourcing arrangements are strategically initiated and managed. (Millward and Brewerton, 1999)	Determining Contractor Behavior/Authority Influences Agency Costs, Employment Conditions/Relationships, Length of Employment, Opportunistic Behavior, Transaction Costs
A relational psychological contract is more likely to foster attachment to employer, not just remuneration-based. (Millward and Brewerton, 1999) (Socially based on trust, stability, long-term commitment)	Employment Conditions/Relationships, Length of Employment, Opportunistic Behavior, Transaction Costs
Transactional psychological contract characterized by short-time frame and attitude of limited organizational contribution, low commitment, weak organizational integration/identification, attitudes of limited flexibility and easy exit. (Millward and Brewerton, 1999)	Employment Conditions/Relationships, Length of Employment, Opportunistic Behavior, Transaction Costs, Loyalty, Ethical Flexibility

It should be no surprise that information technology professionals often contain a set of personal properties that reflect modern social context in a computer dependent environment. This set of literature studies the human aspect of existing conditions pertaining to IT which management should include in decisions to outsource IT. This literature also supports Willcocks and Lacity's (1995) account of the IT environment being a special case when it comes to making outsourcing decisions. A second hypothesis emerged: *Psychological aspects, such as typical IT professional personality traits of today's information technology employees and employee loyalty, are major contributing factors to the potential of insider threat*, suggests that there are significant factors that must be considered as crucial to the outsourced IT and the insider threat phenomenon.

The properties of the Psychological Factor category are summarized in Table 7:

Table 7: Psychological Properties

Psychological
Personality Traits **Loyalty** **Technological Culture** **Employment Conditions/Relationships** **Opportunistic Behavior** **Length of Employment** **Transaction Costs** **Ethical Flexibility** **Interpersonal Social Frustrations** **Computer Dependency** **Triggers** **Economic Trends** **Internationalization** **Agency Costs** **Opportunity/Motive** **Social Trends** **Emotional Needs/Power/Revenge**

Social and Economic Elements of Information Technology and Outsourced Systems

This category is primarily described by the properties of internationalization, social trends, IT culture, loyalty, and employment conditions/relationships. Situations related to the global economy and increased internationalization include trends such as increased business with foreign governments, and an influx of foreign students and workers in high technology fields.

The second-level perspective of category properties is presented in the Table 8:

Table 8: Second Level Perspective of Social and Economic Category and Properties

Socio-Economic Elements of IT Outsourcing	Properties
Technological advances decrease ability to control distribution of sensitive information (Heuer, 2001)	Technological Trends
Changes in industry have placed personnel involved in sensitive military R&D and production in official business contact with people in foreign countries that are conducting espionage against the U.S. (Heuer, 2001)	Internationalization, Anti-American Sentiment, Social Trends, Outsourcing Trends
Sense of loyalty among employees eroded by: downsizing, outsourcing, transferring of jobs overseas, restructuring to accommodate global economic competition, rapid technological change, increased hiring of part time employees. Decreased Job Security. (Heuer, 2001)	Loyalty, Ethical Flexibility, Internationalization, Outsourcing Trends, Technological Trends, Employment Conditions/Relationships,
Cases reveal complex issues of loyalty in an international environment (Shaw et al., 1998)	Internationalization, Loyalty
Sense of loyalty among employees eroded by: Increased internationalization of high tech fields, conflicting loyalties due to increased number and variety of countries conducting intelligence operations against the U.S. (Heuer, 2001)	Loyalty, Ethical Flexibility, Internationalization, Social Trends, Anti-American Sentiment
½ of all doctoral degrees in physics, chemistry, and computer science go to foreign-born students. (Heuer, 2001)	Loyalty, IT Culture, Internationalization
Increased dependence on information systems (Shaw et al., 1998; Zaiton, 2000; Magklaras and Furnell, 2002)	Computer Dependency, Technological Trends, IT Culture
Societal trends toward ethical flexibility found by researcher to be result of lack of specific computer-related ethical training and lack of regulations w/in organizations = lax employee ethical attitudes. (Shaw et al., 1998)	Social Trends, Ethical Flexibility, Technological Culture
Societal trends of cross-generational ethical flexibility found by researchers to be result of lack of ethical training in schools and at home by parents (Shaw et al., 1998)	Social Trends, Ethical Flexibility
Current controversy over H1B visas, raising of cap, unemployment among citizens in high-tech fields, and uncounted and untracked laid-off H1B foreigners remaining in country (Swartz, 2001)	Internationalization, IT Culture, Social Trends, Economic Trends, Ethical Flexibility
Computer industry implicated in erosion of ethical standards (software restrictions, hiring of former hackers). (Shaw et al., 1998)	Ethical Flexibility, IT Culture

Growing trend is joint ventures between India and U.S. computer companies – India supplies U.S. firms with UNIX operating systems, motherboards for high-end workstations, and complete workstations; U.S. government agencies' software maintenance contracts also contain applications written and maintained by Indian programmers. (Keeler, 1997)	Internationalization, Social Trends, IT Culture, Loyalty, Computer Dependency, Technological Trends, Outsourcing Trends
Professional employees tend to be more committed to their profession and its values than to their employers. (Mueller and Wallace, 1992)	Loyalty, Employment Conditions/Relationships, Opportunistic Behavior
Influx of H1B workers (capped at 115K/year), nearly half from country of India (Ruber, 2000)	Technological Culture, Social Trends, Economic Trends, Internationalization, Employment Conditions/Relationships
Influx of H1B workers (capped at 115K/year) divided as follows: 54% Systems Analysts/Programmers; 5% other IT fields; 5% engineering, 36% other. (Ruber, 2000)	IT Culture, Economic Trends, Internationalization, Employment Conditions/Relationships
Job commitment and intended continuance impact job commitment. (Hodson and Sullivan, 1985)	Employment Conditions/Relationships, Loyalty, Opportunistic Behavior

Internationalization and loyalty are properties of concern due to social trends. These properties not only apply to mixed loyalties between countries of origin and the United States, but also between high-tech workers whom believe they are losing work and educational opportunities to the foreign markets. These factors present opportunities for insider threats to information technology not just from a foreign source, but a growing threat from disgruntled domestic sources as well. From this analysis comes a third hypothesis: *Social indicators such as increased foreign influence and growing anti-American sentiment worldwide potentially increase the insider threat risk*.

The Social and Economic category properties are summarized in Table 9:

Table 9: Socio-Economic Properties

Socio-Economic
Internationalization **Ethical Flexibility** **Social Trends** **IT Culture** **Loyalty** **Employment Conditions/Relationships** **Economic Trends** **Outsourcing Trends** **Technological Trends** **Opportunistic Behavior** **Computer Dependency** **Anti-American Sentiment**

Systemic Elements of Outsourcing, Practices, and Insider Threat

The last category of data analyzed for patterns involves not only managerial conditions and effects of decision-making, but operational practices and impacts in today's modern, interconnected, global environment. The elements that led to the properties extracted from this literature, while probably not revelations in the information or industrial security fields of expertise, may assist management in future outsourcing IT considerations. It is generally understood that, "You can outsource the work, but you can't outsource the risk," according to Jay Ehrenreich, senior manager for cyber crime prevention and response, PricewaterhouseCoopers (Schwartz, 2003). Risk is an inherent part of any decision-making process. It is intended this analysis will aid in more comprehensive risk analysis or threat detection in future outsourcing endeavors.

It is also no surprise that access and personnel security practices are perceived to be among the top concerns of data elements comprising this category. IT culture is indicative of a society of people dependent on computers and information where loyalty and ethical flexibility are now quite logically some of management's top concerns, especially when considering whom will be in charge of an organization's critical information and systems. Finally, social, economic, and technological trends in the environment outside the organization as well as the employment conditions within the organization will have significant bearing on how concerned employees will be with protecting information.

The second-level perspective of the systemic category and its properties are shown in the next table:

Table 10: Second Level Perspective of Systemic Category and Properties

Systemic Elements of IT Outsourcing	Properties
Major investments are devoted to technology to detect and prevent external intrusions; human problem is often not as significantly explored. (Shaw et al., 1998)	IT Culture, Information Distribution, Access, Economic Trends, Management Practices
Information Systems are most vulnerable to those who know system best (insiders) due to unbalanced approach to system security (Shaw et al., 1998)	Access, IT Culture, Personnel Security Practices, Management Practices
Background investigations are often higher priority for staff employees than contractors, consultants, or temporary workers whose roles are more transient and are not vetted in organization. (Shaw et al., 1998)	Access, Information Distribution, Personnel Security Practices, Management Practices
Cases reveal complex issues of loyalty in an international environment (Shaw et al., 1998)	Loyalty, Internationalization
Increased dependence on information systems (Shaw et al., 1998; Zaiton, 2000; Magklaras and Furnell, 2002)	Computer Dependency, IT Culture, Social Trends

Cases reveal high incidence of former employees to be insider risk if they retain access (directly - backdoors or indirectly - associates); can install backdoor access if anticipating termination/layoffs (Shaw et al., 1998)	Employment Conditions/Relationships, IT Culture, Personality Traits, Personnel Security Practices, Access, Ethical Flexibility, Uncertainty
IT Trend contributed to increased vulnerabilities over last decade: "elimination of need-to-know principle" (increased information sharing). (Shaw et al., 1998)	Information Distribution, Access, IT Culture
Clearance Backlog (DSS, 2001) in Aug 2000 (per GAO) for defense, civilian, and contractor personnel was approximately 505,000 plus cases. As of Feb 2001, DSS could still not verify number of backlogged cases.	Access, Information Distribution, Personnel Security Practices, Uncertainty
Contractor Misconduct (Lunney, POGO, 2002) Top government contractors repeat criminal offenses, pay approx. $3.4 billion in fines, penalties, however, do not get debarred or suspended.	Outsourcing Trends, IT Culture, Personnel Security Practices, Access, Ethical Flexibility, Management Practices
Briefing memo from J. Vincent Chase preceding the hearing on security investigation/clearance backlog, "The purpose of a personal security investigation is to determine an individual's loyalty to the United States, character, trustworthiness, honesty, reliability, discretion, and judgment are such that the individual can be expected to comply with government policy and procedures for safeguarding classified information" (DSS, 2001, p. 3).	Loyalty, Personality Traits, Personnel Security Practices, Access, Ethical Flexibility
Factors affecting clearance granting: "Allegiance to the United States; foreign influence; sexual behavior; personal conduct; financial consideration; alcohol consumption and drug involvement; emotional, mental, and personality disorders; criminal conduct; security violations; outside activities; and misuse of information technology. (DSS, 2001, p.5)	Loyalty, Ethical Flexibility, Personality Traits, Internationalization, IT Culture, Access

A fourth and final hypothesis, *Systemic factors such as outsourcing trends and personnel security practices potentially increase the insider threat*, can be indirectly supported by the properties that were from all categories of literature. Outsourcing trends, however, are an indirect contributor, as management sometimes has no choice but to outsource gaps in resources and capabilities, as stated in Resource Based Theory

(RBT). Resource Dependency Theory (RDT) also claims that every organization will need to depend on another for certain resources, skill, or capabilities. The systemic category of information is related to access to critical information and systems, and it is only logical to assume that outsourcing a system does increase access and personnel security concerns.

Therefore, the outsourcing trend must be addressed in terms of mitigating risks brought about by granting access to outsiders as they become insiders. This also brings the focus of this integration of literature to the workplace within the organization – the source of insider access, management practices (whether hiring, outsourcing, or firing), and security practices (operational or personnel). This focus on the organization will be shown in the final model.

Table 11: Systemic Properties

Systemic
Access
IT Culture
Personnel Security Practices
Loyalty
Ethical Flexibility
Internationalization
Social Trends
Outsourcing Trends
Employment Conditions/Relationships
Uncertainty
Economic Trends
Management Practices
Computer Dependency
Information Distribution

Relationships Between Category Properties

Table 12 gives a concept-centric view of the property relationships. Tables four, five, six, and seven indicate the elements believed to be representative of their respective categories. In showing the relationships between properties drawn from the literature and data in the four categories coded above, it was first noted that some categories shared many of the same properties. The best way to view the relationships between the categories and properties was to construct a model, based on information from table12:

Table 12: Category Property Relationships

Category / Property	Outsourcing Theory	Socio-Economic Factors	Psychological Factors	Systemic Factors
IT Culture	X	X	X	X
Employment Conditions/Relation	X	X	X	X
Economic Trends	X	X	X	X
Internationalization		X	X	X
Opportunistic Behavior	X	X	X	
Ethical Flexibility		X	X	X
Loyalty		X	X	X
Social Trends		X	X	X
Computer Dependency		X	X	X
Technological Trends	X	X		
Transaction Costs	X		X	
Agency Costs	X		X	
Information Distribution		X		X
Outsourcing Trends		X		X
Uncertainty	X			X
Contract Complexity/Length	X			
Resource Gaps	X			
Measured Outcomes	X			
Resource Dependency	X			
Core Competencies	X			
Risk	X			
Disaster Recovery	X			
Organizational Culture	X			
Anti American Sentiment		X		
Personality Traits			X	
Interpersonal Social Frustrations			X	
Length of Employment			X	
Opportunity/Motive			X	
Emotional Needs/Power/Revenge			X	
Triggers			X	
Personnel Security Practice				X
Access				X
Management Practices				X

The first step in constructing the model was to identify the overarching properties of all four categories. These are the antecedents or preconditions, shown in Figure 5, that guide the events or situations depicted by the interaction between model constructs.

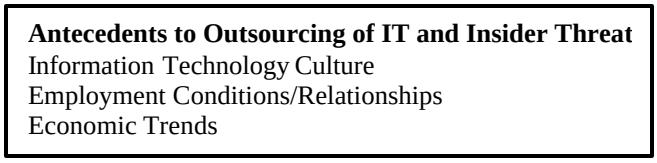


Figure 5: Preconditions for Outsourced IT and Insider Threat

IT Culture, Employment Conditions and Relationships, and Economic Trends: Preconditions of the Model

There are many factors driving the shifts in IT culture as it pertains to information. The integration of information and its associated technology, tangible and intangible, into everyday life has not only changed the way business is done, but has had social effects. Relationships are built, fostered, and sometimes destroyed over the Internet. It has created many jobs, but cost some as well. It has made work faster and more efficient in many organizations. However, there are questions as to whether productivity has increased as a result of massive economic trends in IT investments.

IT culture has brought with it in the last decade an entirely new category of careers, literature, professional organizations, educational and degree programs, as well as its own vocabulary. It has also brought with it its very own flavor of crime and rogue or deviant behavior. Economic trends of Internet shopping, banking, financing, investing, and trading have opened opportunities for extraordinary numbers of identity

theft cases. Unstable relationships in organizations have resulted in vengeful hacking behavior, intrusions, malicious codes and sabotage, denial of service attacks, and intellectual property theft. Interpersonal work conflicts are settled by wreaking havoc on core assets – information. The federal government has stood up entire departments made up of professionals dedicated to securing our information and the equipment that manages it.

These cultural and economic shifts can be viewed from both positive and negative angles. However, they must be acknowledged as catalysts for larger economic, social, and even psychological issues that now confront establishments, directly and indirectly, on many levels.

Model Constructs

Figure 6 shows the category and property relationships that emerged from the data analysis.

The categories of information are depicted in the model by the boxes with the bold outlines. These are the major model constructs and each of their respected boxes lists properties not shared with other categories.

The smaller boxes show the relationships between the categories and those properties shared by the connected categories.

Model analysis will begin with the main categories, followed by exploration of the relationships between the categories as defined by the extracted properties.

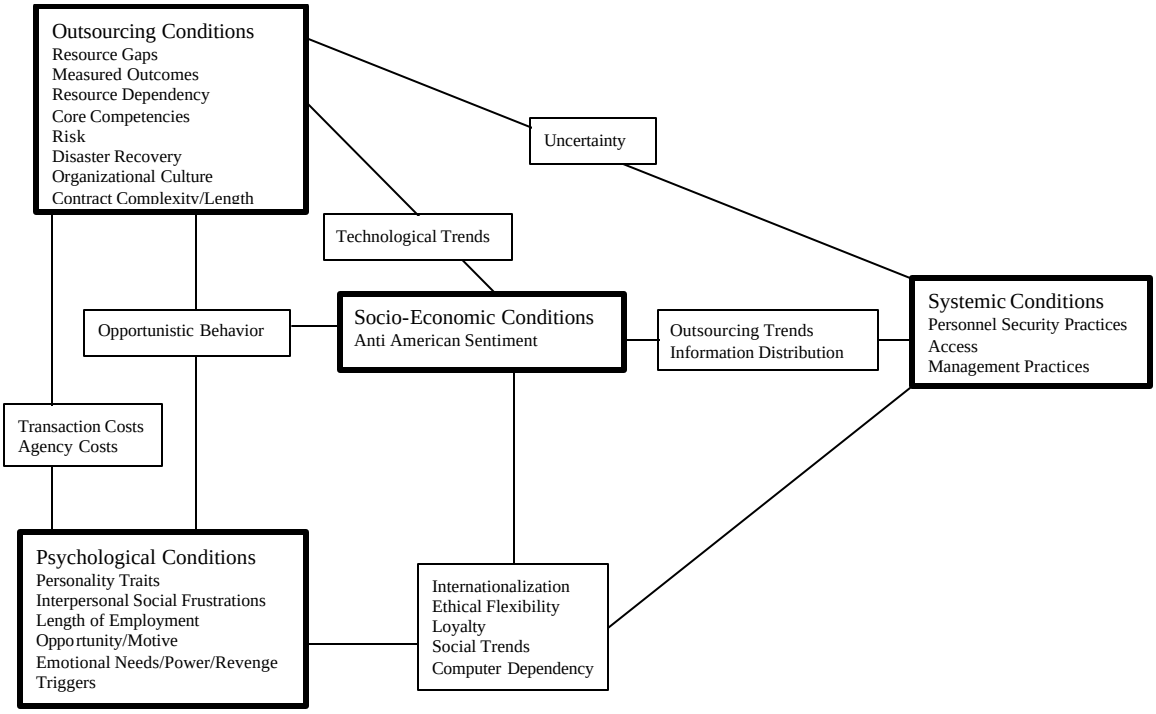


Figure 6: Outsourced IT Insider Threat Model

Unique Properties to the Four Major Categories

Outsourcing Properties

The properties descriptive of the outsourcing construct center around the conditions that are present while undergoing a process that involves considering, researching, writing, or recovering from a contracted effort.

Resource Gaps

In Chapter Two, resource gaps are mentioned as a primary reason to engage in contracting out. Deficiencies in technological capabilities, assets, or skill sets are addressed under the Resource Based Theory (RBT) of outsourcing. When a company

requires these resources to maintain or gain a competitive edge, a viable option is to outsource. Information technology and associated skills are outsourced to fill requirements an organization does not have the capability to staff in-house (Lacity and Hirschheim, 1994; Cheon et al., 1995; Tayntor, 2001).

Measured Outcomes

These are factors that require specific results from a contractor, such as producing a certain quantity or processing a minimum number of jobs. Measured outcomes also require more stringent contract requirements and may drive up the cost of negotiating, writing, and monitoring the contract, in order to maintain control over the process (Cheon et al., 1995; Antonucci et al., 1998; Tayntor, 2001).

Resource Dependency

Referencing back to the Resource Dependence Theory (RDT) in Chapter Two, RDT posits all organizations must depend on other organizations for something (Cheon et al., 1995). Outsourcing is a strategy used to access technologies, services, or other resources not intrinsically available to the organization.

Core Competencies

Those items unique to an organization are not usually considered for outsourcing. Information technology is not often seen as a core competency; IT is a function viewed as imitable by other providers (Cheon et al., 1995). However, in the case of the information that rides the IT systems, trade secrets or other proprietary information could possibly be viewed high-value information to the firm that gives it the competitive edge – if they are kept secret (Mata and Fuerst, 1995). It is also true of National Security information and

the systems that can be considered "centers of gravity" to a network centric warfare environment.

Risk

As mentioned earlier, risk is inherent in the decision to outsource due to potential loss of control, IT security, and flexibility (Fink, 1994; Jurison, 1995; Antonucci et al., 1998; Tayntor, 2001). Resources must be allocated in such a way to avoid over-investing "in certain measures to stem certain risks while paying inadequate attention to others" (Rumsfeld, 2002, p. 23). Outsourced IT concerning the DoD could result in lack of security, flexibility, and control contributes to "Institutional Risk," which Secretary Rumsfeld states is a result of "factors affecting the ability to develop management practices and controls that use resources efficiently and promote the effective operation of the Defense establishment" (2002, p. 23).

Another kind of risk concerning outsourced IT is "Operational Risk." Kliem (1999) professes this type of risk stems from such behaviors as: "becoming too dependent on a vendor for mission critical services; being unable to determine the quality of the service being delivered; … having a vendor fail to provide an adequate level of services" (p. 3). These factors are directly related to the DoD's ability to carry out mission objectives if a vendor is not performing as required. Secretary Rumsfeld addresses the operational category of risk in the DoD's risk management framework: "Operational risk stems from factors shaping the ability to achieve military objectives in a near-term conflict or other contingency" (2002, p. 23). The risks of undermining the efficiency of military operations are present in the decision to outsource IT.

Disaster Recovery

Risk and disaster recovery can be thought of in the same ilk of management concerns when pursuing outsourcing options. According to Jurison (1995), "The dominant risk is the irreversibility of the decision" (p. 240). Jurison also found that if an outsourced IT function does not work out, it could be "very costly and difficult to bring the work back into the firm" (p. 240). Fink's (1994) Security and Control Framework for Outsourced Information Systems (IS) contains a business recovery component that encompasses all other components of the model:

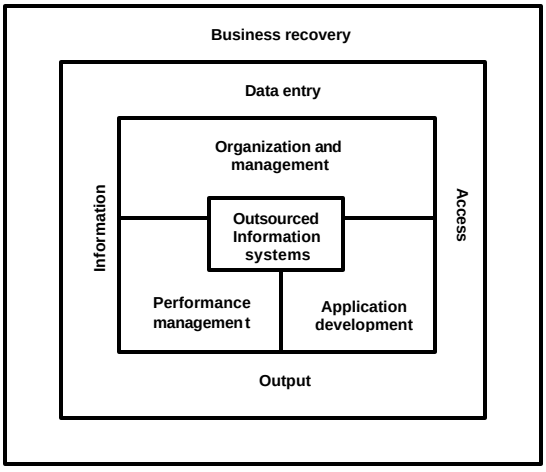


Figure 7: Security and Control Framework for Outsourced IS (Fink, 1995)

Fink examines security risks in outsourcing and explains the need for an organization to "ensure continuity of business activities very carefully by identifying threats, devising counter-measures, and having procedures in place to overcome disasters

should they occur" (p. 6). The key to Fink's model is that disaster recovery should be a first line consideration to all other factors in outsourcing information technology systems.

Organizational Culture

An organization with processes embedded in a complex social structure will find it naturally resistant to change, and according to Mata and Fuerst (1995) costly to change when it comes to outsourcing IT. Mata and Fuerst's resource-based analysis of IT's role in an organization's competitive status "reflect the unique histories of individual firms, are often part of the "taken for granted" routines in an organization, and can be based on socially complex relations within the IT function, between the IT function and other business functions within a firm, and between the IT function and a firm's suppliers or customers" (1995, p. 499).

Because of the social complexities of organizations with strong cultures, effects of outsourcing on employee morale can be negative (Kliem, 1999) due to expected layoffs or displacement of IT talent to the vendor (Antonucci et al., 1998). The social structure and behavior patterns of employees within the organization can be affected. Employees may become concerned that management is concerned only for the organization and not the employees, possibly resulting in a less trusting environment. Outsourcing IT is often "fraught with emotional arguments, difficult questions and complex links with many organizational processes" (Clark et al., 1995).

Contract Complexity/Length

Writing a more complex contract of course drives the cost. However, in order to determine specific behaviors or performance standards desired by the contractor, it is sometimes necessary. Recall that bounded rationality impacts the extent of contingency

planning, risk aversion, and disaster control that can be written into the contract. The higher the uncertainty and risk aversion considerations in an outsourcing endeavor, the higher the contract agency costs will be. The same applies to longer contracting relationships (Cheon et al., 1995).

Psychological Properties

Those properties found primarily in the Psychological Conditions construct pertain to individuals involved in the information technology environment. These properties are presented as resulting from the proliferation of an interconnected computer environment, the outsourced IT environment, or a combination of both. The significance of these properties is that they are potential indicators of who may be a security risk, and why.

Personality Traits

A blend of personality traits that were considered "direct implications for risk…" (Shaw et al., 1999, p. 2) all focused around an individual's being more in tune with computers than people. They are unable to successfully resolve issues in the work place, easily frustrated, and in spite of low self-esteem, and are narcissistic or view themselves as "special and owed corresponding recognition, privilege, or exception" (Shaw et al., 1999, p. 4). These characteristics are seen as risks due to a corresponding quickness to disappointment or anger, manifest their negative feelings in the form of computer-based actions such as e-mails, or even attacks.

Shaw, Ruby, and Post also found "Every psychological assessment of programmers, computer scientists, computer science graduate students, and systems

administrators has found one common trait: introversion" (1999, p. 2). This trait carries with it the same implications of behavioral patterns previously discussed.

Interpersonal Social Frustrations

Along the lines of the personality trait of introversion, computer professionals have a tendency to replace human relationships with computers (Shaw et al., 1999). Social frustrations also manifest themselves in hatred for authority and vengeful behaviors. Shaw, Ruby and Post's research also found that a significant population who chose the computer science profession as a result of their inability to relate to other people (1998).

Length of Employment

Millward and Brewerton (1999) found that although it is feasible that contractors can be productive and loyal employees, there exists speculation that, "An emotionally-detached and self-interested employee who fails to become integrated into the organizations is one whose commitments and energies are likely to be focused elsewhere" (p. 256).

Short-term employees may not see their current employment situation as an opportunity for growth or professional (or personal) development, therefore, reducing level of commitment. Due to their transient nature "a lesser degree of loyalty to the firm or agency would be anticipated" (Shaw et al., 1998, p. 5) from short-term employees, such as contractors or subcontractors. The longer an employee stays (or intends to stay) with an organization the more loyalty has a tendency to increase (Mueller and Wallace, 1992).

Opportunity

Opportunity for betrayal by an insider has increased with easier access to information in an interconnected environment; with that opportunity comes temptation (Heuer, 2001). Not only is it easier to access data, it is easier to transmit it without detection. Heuer also points out increased opportunity for foreign contacts due to industry trends:

> …where personnel involved in sensitive military R&D and production are increasingly in official business contact with their counterparts in foreign countries that are conducting espionage against the United States. The line between military and non-military, and between classified technology and unclassified technology sold to foreign countries, is increasingly blurred (2001, p. 3).

Motive

Like opportunity, motive is also a precondition for negative insider behavior. Motivations can be intrinsic, such as emotional needs (discussed below) toward goals of increased self-esteem. Motives can also be financial, or a combination of both (Heuer, 2001), such as events in the work place resulting in "disgruntled employees who are angry about lay-offs, transfers, and other perceived grievances" (Shaw et al., 1998, p. 2).

Non-malicious insider behavior can stem from curiosity, where the intruder was granted unnecessary access; Shaw, Ruby, and Post refer to curious people with no harmful intentions as "explorers" (1999). Other types that explain motivation behind insider behavior include the individuals that feel they are gifted or special, similar to the character trait of narcissism mentioned earlier; this motivational type is termed "exception" (Shaw et al., 1999). The Regan spy case is a prime example of someone who was financially motivated, but also believed he was entitled to more than he was

getting paid. The result was his writing letters to the leaders of Iraq, Libya, and China, offering to sell classified satellite photos for $13M (McNulty, 2002).

Emotional Needs, Power, and Revenge

The Regan spy case can also be considered an example of revenge-seeking behavior against an agency, in this case, the intelligence community, for not meeting his needs, emotional, financial, or otherwise. Disgruntled employees, whether current or presently on staff, are a "principal source of computer crimes" (FBI, 2000, p. 2). There are many cases where an insider uses the power of system access and known vulnerabilities to "get back" at losing a contract or getting laid off. Installing backdoors, Trojan horses, and logic bombs, as well as deleting files, are all very common methods of using the power of insider knowledge for revenge.

Triggers

Triggers are another of Heuer's (2001) precondition for insider crimes besides opportunity and motive. Compounded by personality traits discussed previously, triggers are simply the event that causes an employee to cross the line into undesired insider behavior. It is posited that individuals displaying the character disorders or personality traits discussed above may have more of a tendency toward betrayal that can be "triggered by some event in the individual's personal or professional life that pushes stress beyond that person's breaking point" (Heuer, 2001, p. 4).

Finally, besides opportunity, motive and triggers, Heuer considers reduced inhibitions such as ethical flexibility and unstable loyalty (to be discussed later) to complete the list of preconditions for insider crime. He also states, "The prevalence of these four conditions is influenced by changes in social and economic conditions in the

United States and in our relations with the rest of the world" (2001, p. 4). This statement leads to the next section that discusses the Socio-Economic properties related to these preconditions, traits, and characteristics.

Socio-Economic Properties

The primary property unique only to the Socio-Economic category is that of Anti-American Sentiment. As the previous section indicated, U.S. relations with the rest of the world will have some bearing over the social interactions, trends, and psyches of people who create, process, transmit, and dispose of information and its associated technologies.

Anti-American Sentiment

Anti-American Sentiment is not restricted to those outside the United States. Due to the modern geographically immune nature of information, the business community is more prolific than ever in a global setting. As a result of "internationalization of many high technology fields, combined with the increased number and variety of countries conducting intelligence operations against the United States" (Heuer, 2001, p. 3), combined with increased joint IT ventures with overseas companies, especially in third world countries (Keeler, 1997), the U.S. may have opened its cyber borders beyond control.

Outside our borders, however, there is a definitive trend in how the world community views the U.S. A recent survey by Pew Research Center entitled, *What the World Thinks in 2002*, showed that "since 2000, favorability ratings for the U.S. have fallen in 19 of the 27 countries where trend benchmarks are available" (Pew, 2002, p. 1).

According the 2002 Pew report, science and technological advances are admired by world majorities (with the exception of Russia); however, there is an overwhelming rejection of "the wide diffusion of American ideas and customs" (p. 63). Americans continue to believe the rest of the world welcomes our cultural influences, and that we are benefactors to the world. The global opinion is not conducive to "the spread of American influence and often say the U.S. creates more problems than it solves" (p. 70).

This concept is crucial to understanding that Americans less accepting of foreign culture have obstacles to overcome in a global market where our values are being seen as forced on others. This concept of Anti-American sentiment is an important consideration in the information technology environment where loyalty, whether it be American or another nation's, can impact the threat potential.

Systemic Properties

Personnel Security Practices

This was covered extensively in the literature review in Chapter Two. However, it is a critical factor in controlling who is accessing critical information systems. This is especially important when considering outsourcing IT systems, given the potential threat posed by those armed with critical system knowledge. It is important to know who is using, managing, operating, and maintaining IT.

According to a 2002 NASA IG report:

> Our audit, Approvals for Accessing Information Technology Systems (IG-02-004), found that two NASA installations did not complete required security investigations for all personnel who accessed sensitive IT systems. In our test sample, we found that one Center completed security investigations for less than 20 percent of contractor

> employees who were accessing sensitive IT systems. At the other Center, we found that temporary employees with access to sensitive IT systems did not receive required security investigations. (NASA, 2002, p. 5)

Not only do employees, including contractor personnel, require screening, levels of access concurrent with personnel duties should also be determined and enforced.

Access

The protection of information was once protected by physical means, such as safes and locked doors. It is more difficult to control access to data that rides on public infrastructure, or that is accessed by more people due to outsourcing.

Modern day protection "focuses on protecting information systems and data from accidental or intentional unauthorized access, disclosure, modification, or destruction" (Loch, 1992, p. 173). Public key infrastructure, for example, is a modern method of controlling access that only allows certain actions to be performed by a key holder.

Management Practices

While securing the facilities, screening personnel, and controlling access are all part of keeping information secure, management must also implement prescribed security procedures, enforce controls, and efficiently deal with breaches.

Firing people also has its security concerns. Individuals who know they are targets for outsourced or downsized functions are sometimes apt to sabotage data or delete records, install logic bombs, or trap doors in the systems they can access from outside the company. Management must ensure when engaging in drastic personnel and organizational changes, that passwords and access privileges are reviewed for all concerned. Referencing back to the section on disaster recovery, management should be prepared for any attacks by disgruntled or former employees.

Relationships Between Categories

There were properties shared between three categories, two categories, and some properties unique to one category (covered by the previous section). This section describes the interactive relationships that occur between properties.

Psychological, Socio-Economic, and Systemic Conditions

The most collective grouping of properties shared by the psychological, socio-economic, and systemic categories, shown in Figure 8:

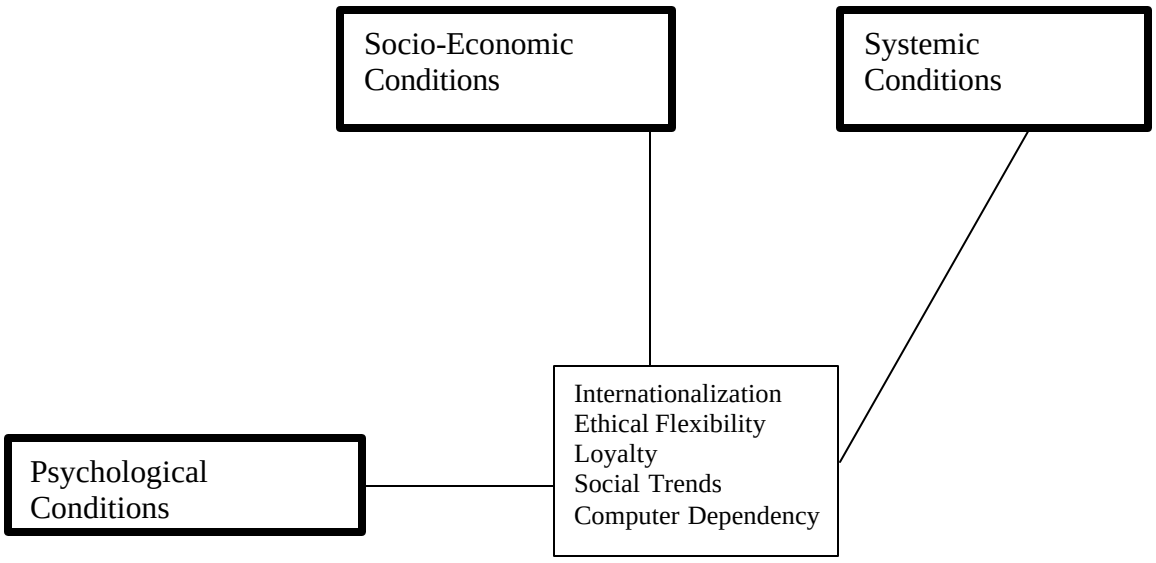


Figure 8: Common Properties of Psychological, Socio-Economic, and Systemic Categories

Internationalization

This is a term referencing the global economy and business market activity. People from many countries, cultures, and beliefs are connected through technological advances that bring economic and social issues into focus in a media rich environment. Technology trends have given organizations the ability to conference globally and

coordinate business transactions and plans online. International relationships are becoming the norm, organizationally and socially.

Another aspect of internationalization involves the influence foreign-born persons have had on our education and employment systems. As mentioned earlier in the literature a large portion of graduate degrees awarded in the United States are to students from other nations (Heuer, 2001). Furthermore, highly technical fields have seen an influx of international workers through the H1B visa and other programs.

Internationalization is making it harder to draw clear borders between countries in the interconnected global environment. U.S. businesses have established offices globally, and other countries have brought their companies to the U.S. It is also with this trend of internationalization that conflicting loyalties between countries may become an issue (Heuer, 2001).

Ethical Flexibility

The relationship between the Psychological, Socio-Economic, and Systemic categories also includes the property of ethical flexibility. As a result of a computer dependent society, it is possible that it is becoming more difficult for many people to realize the overall impact of their keyboard strokes or mouse clicks. Work by Shaw, Ruby, and Post mentions this type of ethical flexibility with respect to the computer work environment as well as cross-generational lack of training and guidance in schools and at home by parents (1998).

High-tech workers have expressed concern that job security is at risk, fearing displacement due to influxes of H-1B visa workers (capped at 195,000 per year); H-1B visa workers are often reported to be paid one-third less than American workers. "With

layoffs rising, paranoia and distrust set in, not only between Americans and foreigners, but between different workers, too" (Swartz, 2001, p. 4). This type of environment has resulted in disgruntled American workers who harass, threaten, and demoralize foreign workers (Swartz, 2001), sacrificing and ethics in the work place for fear of being laid off.

Loyalty

Employee loyalty has been examined in this research not only from the individual psychological perspective and the IT personality profiling but also from the perspective of contracted employment. Conditions in the social and organizational environments in the workplace can determine loyalty an employee may have for his employer. The effects of short-term employment contracts can logically have an effect on loyalty when an individual is not integrally identified with the organization (Millward and Brewerton, 1999). One can look at the Socio-Economic situations common in the news about Enron and other companies costing employees their retirement to hypothesize whether employee loyalty has been shaken on a larger scale.

Social Trends

Social trends, not only in the international environment, but amongst computer users and professionals, have had a certain impact on the psyches and relationships in the high tech work environments. Social situations in other countries have driven Indians and Chinese (among others) to the United States to pursue education and employment under the H1B visa program. However, in a post "September 11th" environment especially, H1B visa holders have become the victims of "threatening notes, demanding that Indian workers 'go home'" (Swartz, 2001). It is becoming more commonplace for tensions between American and foreign workers to rise as studies by major universities

such as University of California at Los Angeles (UCLA) and Cornell found H1B visa workers were being hired at 20 to 33 percent lower wages than Americans in the same fields.

Other social trends among computer users include the constant upgrading that is done to keep up with technological trends. Studies regarding the "productivity paradox" are being devoted to determining whether the investments in computer technology are really paying off in terms of productivity. Personal computer trends have also brought with it a computer-savvy and sometimes dependent generation as well.

Computer Dependency

While entire societies, in the United States and globally, have become dependent on the information that can be rapidly accessed by even more rapidly advancing technology, people have become dependent on computers in a psychological regard as well as cultural. Studies focusing on insiders and IT have shown computer dependency as a personality trait common among deviant insiders. Furthermore, these computer dependent persons turn to computers to fill social needs not being met by relationships with other people, whether informally or at work or school (Shaw et al., 1998).

Outsourcing, Psychological, and Socio-Economic Conditions

This section describes briefly the one property shared by the Outsourcing, Psychological, and Socio-Economic categories, shown in Figure 9:

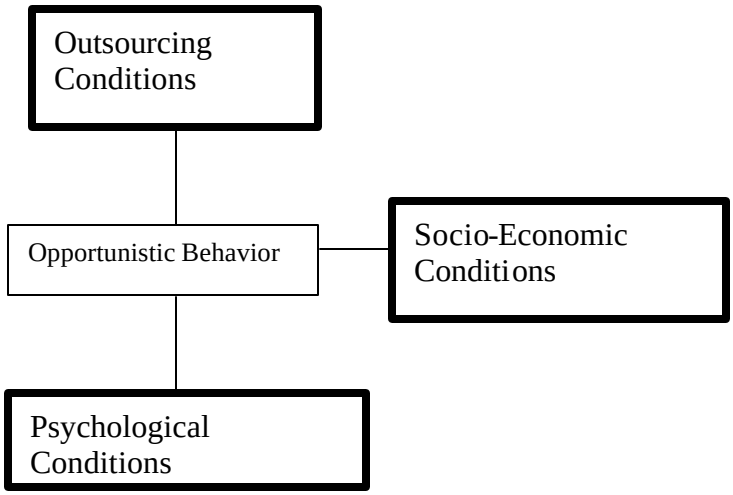


Figure 9: Opportunistic Behavior

Opportunistic Behavior

This property is considered to be a tenet of Transaction Cost Theory (TCT) approaches to outsourcing, in terms of human behavior. The risk inherent to outsourcing due to our bounded rationality and the "assumption that agents, acting in their own self-interest, are subject to opportunistic behaviour" (Jurison, 1995, p. 241) is most certainly human-based. It is this property, driven possibly by employment or Socio-Economic conditions that ties the psychology of the computer-dependent, ethically flexible, and possibly vengeful or narcissistic to the outsourcing risk. It is a substantial connection when looking at insider behavior, especially that of the new generation of IT personalities that have become characteristic of the IT professional and the social conditions of the work environment where outsourcing IT is taking place.

Outsourcing and Psychological Conditions

The main properties shared by these two categories involve transaction and agency costs. This relationship is shown in the Figure 10:

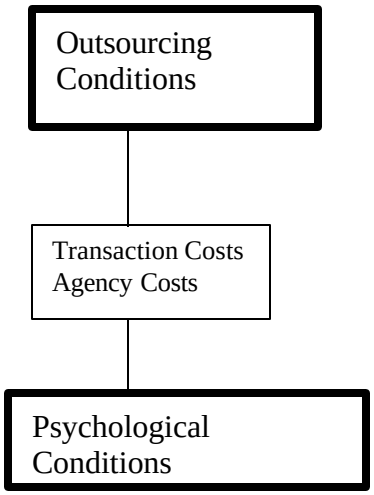


Figure 10: Transaction and Agency Costs

Transactional costs are the costs for those goods and services provided by a vendor (including market research and writing of contracts). This relationship, often short term, may generate a less relationship-based commitment from contractors as Millward and Brewerton examine in their 1999 study. They go on to warn against putting all contractors in the same category as being disconnected from the workplace. Contracted employees are to be considered as people, and not just assets or resources. Millward and Brewerton also found in their study that "it is possible for 'contractors' to be integrated within the workplace on a partnership basis so long as outsourcing arrangements are strategically initiated and managed" (1999, p. 272).

It is the psychology of the IT professional that makes outsourcing IT unique to most other functions. In building that relationship, and attempting to obtain a contract that specifies the desired outcomes and behaviors, the agency costs that are accumulated in the negotiating, litigating, and monitoring of the contract, can increase as the contract becomes more complex. In order to keep certain personality traits of high tech workers (narcissism, or vengeful actions upon contract completion or discontinuance) from manifesting into dangerous insider behavior, contracts must address contingency responses to disasters and security controls, both on the part of the vendor, and on the organization outsourcing its IT.

Outsourcing and Socio-Economic Conditions

The connection between these two categories is more conspicuous. Figure 11 shows the relationship and the common property of technological trends to the Outsourcing and Socio-Economic Conditions categories:

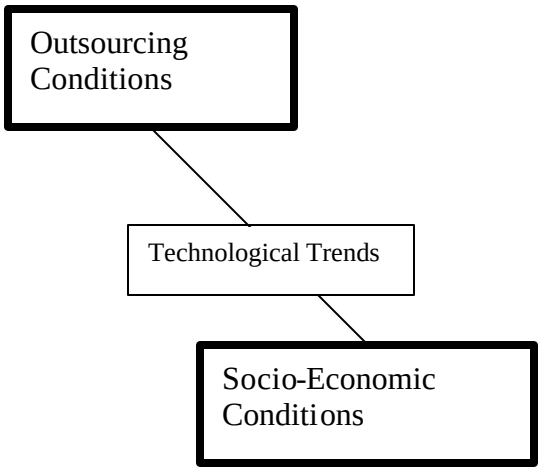


Figure 11: Technological Trends

Technological Trends

Rapid development of technology is an obvious driver in outsourcing. Operating, training, and maintenance costs to keep up with IT trends have given organizations economic and strategic reasons to leave IT to the people who specialize in computer-based technology. Increasing demands on information capabilities of those organizations depending on IT have made IT "one of the most outsourced services" often due to "…shortage of skilled IT staff within most organizations, an inability to cover a rapidly expanding field adequately and the lack of flexibility which can result from over-investment in a particular technology" (Domberger et al., 2000, p. 107).

IT trends have made information a global commodity, fostering socio-economic effects of overseas employment, local downsizing, and outsourcing (Heuer, 2001). Other socio-economic outgrowths of IT trends include: the aforementioned H1B visa program that allows 115,000 people a year from other countries to apply for highly skilled positions in the United States (Swartz, 2001); and growing trends in offshore contracts with software and hardware companies (Keeler, 1997).

Socio-Economic and Systemic Conditions

With trends in technology advancements come trends in outsourcing behavior, as well as trends in widespread distribution of information. Figure 12 depicts these properties and their shared relationship with the Socio-Economic and Systemic categories:

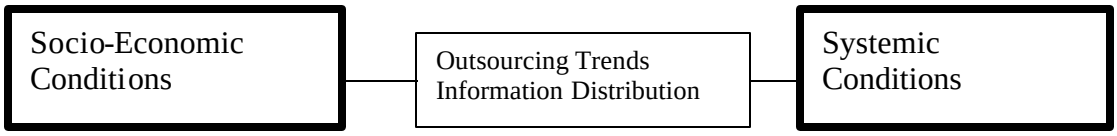


Figure 12: Outsourcing Trends and Information Distribution

Outsourcing trends

Rapid development of technology and capabilities from an organizational standpoint can undoubtedly give rise to the need to fill information resource gaps from outside organizations. Information technology and management of information is often seen as a service than can be easily outsourced in order to reduce costs of training and maintaining to keep up with rapid advancement. If information management is not a core competency or the function that sets an organization apart from its competitors, it is often the case that there are people specializing in IT services who can remove that high tech burden from management. While risk is inherent, there have been many cases where outsourcing IT has proven to be the economically and strategically best option to keep abreast of technological trends (Antonucci et al., 1998; Grover and Ramanlal, 1999; and Tayntor, 2001).

Within the federal government, IT service contracts alone "have increased from $3.7 billion in fiscal year 1990 to about $13.4 billion in FY 2000" (GAO, 2002, p. 6).

Information Distribution

While information distribution has provided a lubricant of sorts to a society that wants (and expects) information at its fingertips, recent focuses in the federal government of the United States have encouraged reconsideration of accessible information. Recent

articles outlining efforts by the DoD to "strip military Web site of information that could benefit adversaries" (Poulson, 2003). According to PERSEREC's Richards Heuer:

> The equivalent of safe-loads of material can be copied in a matter of minutes and transmitted electronically around the globe, often without detection, almost instantaneously…Now, classified and sensitive but unclassified technical information are both stored in large, electronic databases that can often be accessed by large numbers of people with little or no regard for need-to-know. (1999, p. 7)

The perspective that information is becoming harder to control due to technological trends (Heuer, 2001) and trends toward information sharing (Shaw et al., 1998) is also a reality. Peter Drucker, in his book *Post Capitalist Society,* describes information as boundless on a geographic basis, "knowing no country" (1994, p. 143) and that once the information is out, it is impossible to regain control of it.

Drucker also points out that countries all over the world are finding high tech ways to access programming (radio, television, or movie), sometimes forbidden by their governments. Other societies base their opinions on Americans, their values, and lifestyle on the limited programs they can access even if it presents a "distorted" presentation of American culture (1994).

Outsourcing and Systemic Conditions

The property shared by primarily by the Outsourcing and Systemic categories addresses aspects of the work situation where workers are not secure in their futures or roles in the organization.

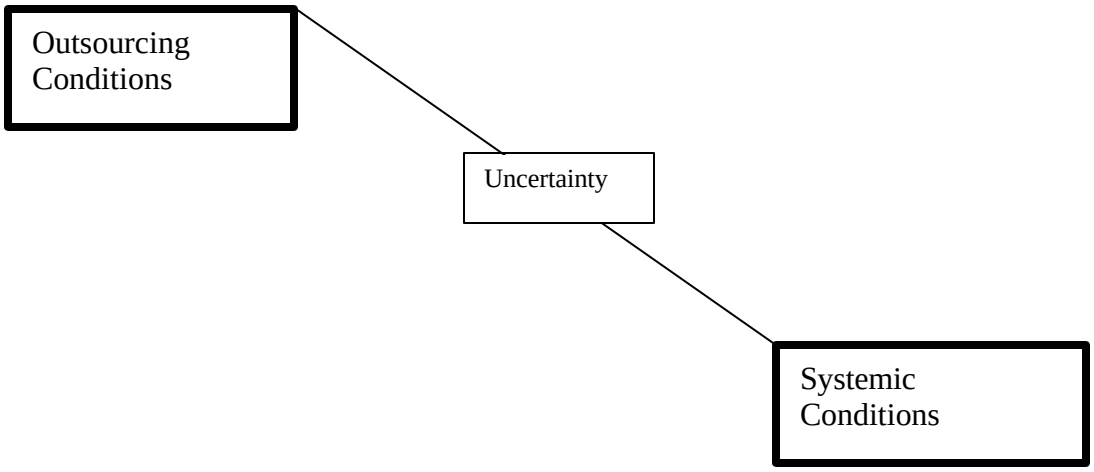


Figure 13: Uncertainty

Uncertainty

This property can be injected into a work environment when employees are not sure if their future with an organization is secure. This is especially true with more frequent downsizing and outsourcing trends in the IT environment, which "often results in layoffs or the transfer of existing employees to the IT vendor. Such displacement can set morale into a tailspin and cause even talented staff to fear for their employment security" (Antonucci et al., 1998, p. 28). Uncertainty can often be injected in the work environment through outsourcing arrangements that leave management and employees feeling loss of control and flexibility of their IT programs and people (Kliem, 1999; Lacity, 2001; and Tayntor, 2001), and lower quality of service (Antonucci et al., 1998) in the desired responsiveness and efficiency required of their IT programs.

Jurison makes the connection of uncertainty to risk in the decision to outsource IT, as management can never entirely predict all of the outcomes and that "humans are unable to foresee the complexities and contingencies in contractual relationships and

consequently can only achieve incomplete contracts" (1995, p. 241). However, stringent inspector general (IG) programs are one effective effort to reducing the uncertainty induced by subcontracting. The National Aeronautics and Space Administration (NASA) IG reported a subcontractor was found and pled guilty to providing false statements documenting the production of faulty parts for the International Space Station and a DoD unmanned reconnaissance aircraft. The parts "contained unauthorized weld repairs. These repairs were not disclosed to NASA or the DoD" (NASA, 2001, p. 48).

In the IT community, some unfortunate results have shown up in subcontracting practices, which have been known to occur without management's knowledge and "cause problems, including viruses brought in by subcontractors, poor communications, high costs and low-quality service" (Antonucci et al., 1998, p. 26). By examining an actual case of insider threat, the next section will explore the complete model and the theory developed.

Model Focus

The theory generated by the concepts and relationships the model that construes the complex phenomenon of the insider threat, the core focus of this research. Figure 14 shows the final model as emergent from the categories and properties.

This model presents not only a theory on insider threat dynamics but presents a case for future monitoring of outsourced IT situations. Indicators to where potential vulnerabilities lie, point to toward workplace controls in security, personnel (contractor and subcontractor) screening, and enforcing of access controls.

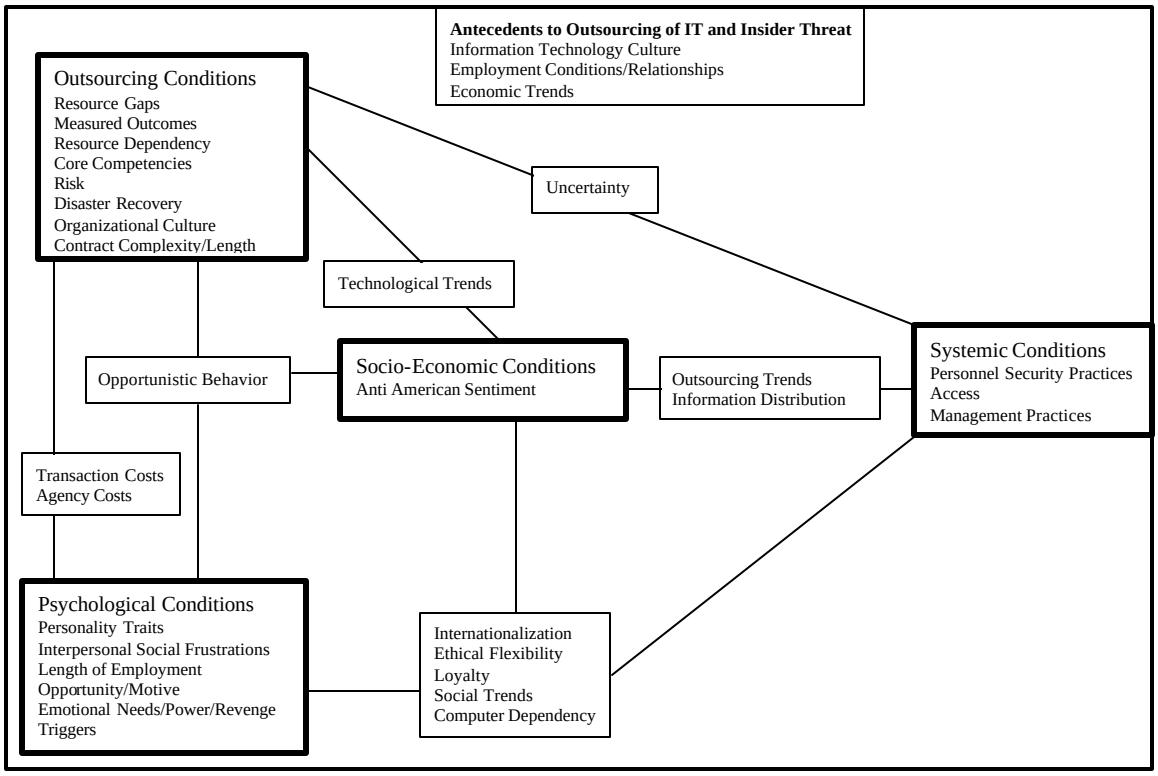


Figure 14: IT Outsourcing and Insider Threat Model

Summary

The final model proposed here shows all four originating categories related to insider threat to outsourced information technology. The properties that have emerged from the data, literature, testimony, proceedings, and cases studied show relationships between the categories, giving the model its conceptual density. The scope of this research only allowed for limited study of outsourcing IT and its impact on the insider threat phenomenon.

Conceptual density of this model can be further achieved, however, by continuing to cross-connect the concepts of this model to gain more insight into the insider threat for predictive purposes. For example, there may be denser cross-connections between the

properties of risk, uncertainty, and information distribution to the Psychological category that could be explored. From this more categories and properties may emerge, giving a better psychological profiling tool for detecting insider behavior as a result of organizational risk-taking. The grounded theory methodology insists continuous cross-connecting of ideas until the model is essentially saturated to achieve pure conceptual density. This is beyond the scope of this research, but may be helpful in future endeavors.

V. Case Study and Model Comparison

Zhangyi Liu Case

This case refers to the incident where Zhangyi "Steven" Liu, a subcontractor, gained unauthorized access to a critical government information system. By reintroducing the model and overlaying the concepts evident in this case, this study demonstrates a high profile situation and the complexity of the insider threat to outsourced information technology within the DoD. The information on the case came primarily from a series of articles published in a local paper, the *Dayton Daily News.*

Liu Case Background

In 1996, a system administrator at Wright Patterson AFB discovered a security breach in the operations side of the Reliability and Maintainability Information System (REMIS) (Gaffney, 1997). REMIS is a $148M logistics system used for tracking aircraft and weapons systems mission capability data, such as maintenance information, missile and communications-electronic information, and aircraft inventory data. Although it is an unclassified system, REMIS "does contain highly sensitive information, both militarily and economically" (Hills and Gaffney, 1997b, p. 1A).

The security breach was by a subcontracted computer programmer, Zhangyi Liu, who was working on developmental software improvements for REMIS. Liu accessed a "super super password" file that contained over 400 REMIS user passwords (Hills, 1999a). He and two other co-workers proceeded to download unauthorized files to a

personal directory that could have potentially been accessed by Internet users, according to an FBI source (Hills and Gaffney, 1997b).

Outsourced Sources

The prime contractor, Litton Industries Incorporated, subcontracted REMIS developmental software work to Muscato Corporation in Florida. Muscato Corp. then subcontracted again to Shanghai Tandem Software Systems, Limited in Shanghai, China. Eleven Chinese citizens from Shanghai Tandem were sent to the Dayton, Ohio Litton office to perform software improvements to REMIS system programs (Hills and Gaffney, 1997b, p. 1A).

Uncertainty of Subcontractor

This second-tier outsourcing practice increased uncertainty and diluted security safeguards for the critical information being maintained on REMIS. The Material Systems Group (MSG) found that due to "Privity of Contract Rights" the government was not allowed to access subcontract information of fixed price contracts. Since then, according to a former MSG executive director, contracts must now require that the use of foreign nationals be disclosed (Hills and Gaffney, 1997b).

Core Competencies and Information Superiority

One of the Air Force core competencies in Air Force Doctrine Document (AFDD) 1 states "the ability to collect, control, exploit, and defend information while denying an adversary to do the same and, like air and space superiority, includes gaining control over the information realm and fully exploiting military information functions" (1997, p. 31).

Liu's possession of the password file, with access to super-level accounts "gave him the power to create, change, or delete any file in the system" (Hills, 1999b, p. 1A). Quoting OSI agent Matthews, "Wood [the system administrator who discovered the breach] was stunned to find the password file, not only to the users of the development system, but also super super accounts and passwords to the operational side of REMIS as well" (Gaffney, 1997, p. 19A). The subcontractors were not authorized top-level access to the development system or any access to the operational system. However, "Liu had gotten both and now he had every top-level password for REMIS at his disposal" (Gaffney, 1997, p. 19A).

When Liu's access was discovered, there was an immediate concern that the contract personnel working on the system, who were Chinese nationals, may have indeed exploited a critical database that tracks aircraft weapons systems data. This was a potential compromising of the integrity of the system and hampering the Air Force's strive toward not only information superiority, but also another core competency – air and space superiority. Air and space superiority "is that degree of dominance that permits friendly land, sea, and air forces to operate at a given time and place without prohibitive interference by the opposing force" (AFDD-1, 1997, p. 29).

Risk, Disaster Recovery, and Costs

Outsourcing decisions concerning IT systems entail the risk of the possibility of a disaster, rendering a system or an organization helpless. In the case of Liu's intrusion, the incident cost the prime contractor, Litton, and the Air Force over $358K to examine code and data to ensure no back doors or malicious code had been installed by Liu or his coworkers. Another $15K was spent to install the missing security patches that allowed

Liu to access the operational side of the system in the first place. This patch was not installed previously due to "funding considerations", according to an Air Force official's reported concession at the hearing (Hills, 1997). Finally, there are no estimates for contract reviews Air Force wide and "costs of investigations by the FBI and the Air Force Office of Special Investigations" (Hills, 2000b, p. 3B).

REMIS Contract with Litton

The contract for the REMIS system was held by Litton, PRC for 11 years, at a cost to the Air Force of $150M (Modic, 1999a). An Air Force official testified at Liu's hearing "he was unaware that Liu and 10 other Chinese nationals were brought in by a subcontractor to debug and improve REMIS' developmental side" (Hills, 1997, p. 1A). Liu's attorneys also stated that the access procedures were never laid out as they were hired to "service the system without ever telling them what they couldn't do" (Hills, 1999a, p. 1B).

Cheap Labor - Opportunistic Behavior

While it is unknown whether Liu was working in the U.S. under the H1B visa program, it is known that he was working for only $500 per month (Hills, 1999a). There is continuing controversy over the hiring of H1B foreign workers by IT companies because they are reputed to work for less money. By cutting labor costs, contractors and subcontractors are able to potentially maximize their profits.

Psychological Background

Not much is known about the personality or behavior characteristics of Liu. His computer programming background, however, may give psychologists a starting point for analyzing personality traits to see if Liu matches the theorized profile of the IT

professional (introverted, narcissistic, computer dependent, etc.) His ethical flexibility, however, did come out during the trial and was self-admitted.

Insight to his motives, however, was revealed by attorneys and investigators involved in the case. What is known about Liu was that he was a bright, successful student who got through college on scholarships. His degree is in electronic engineering from Shanghai Jiao Tong University, where he graduated in 1994. He was "in the top 10 percent of excellent students at the university, according to court records" (Hills, 1999a, p. 1B).

Curiosity as Motive

An initial theory was said to be Liu's curiosity. Being from a poor background, he sent most of his paycheck home to his parents. He told the judge during his trial that he was curious about his performance evaluation because he just wanted to do well in this country. In his search for documented information about his performance, he accidentally found the password file, which was not encrypted with the prescribed patch (Hills, 1999a.).

Emotional Needs and 'The Brass Ring'

Power and perhaps self-esteem needs could have encouraged Liu's behavior once found the password file. Public defender Paul Hensley claimed that Liu's motivation was to "simply 'capture the brass ring' or simply show off to his fellow programmers" (Hills, 1999b, p. 1A). Liu was said to have wanted to impress a female coworker with his access to her password, and reportedly told an investigative agent, "he wanted to own the system" (Hills, 1997, p. 1A). A computer expert testifying as a defense witness at Liu's trial explained the programmer mentality of 'capture the flag', where gaining access to

password files “was a badge of achievement among programmers” (Modic, 1999b, p. 1B).

Ethical Flexibility in an Unsecured System

In addition to the aforementioned stereotypical programmer mentality of ‘capturing the flag’, one could attribute Liu’s neglecting to report the vulnerability to the system administrator to an ethical flexibility trend in computer culture. Liu did mention to one of his attorneys that he was considering trying to access “internal e-mail which might have as its subject an evaluation of his performance” (Hills and Gaffney, 1997a, p. 1A). Liu also admitted that, “he was allowed to walk in a room of secrets. They put the tools in the room without ever telling me not to use them, and just expecting that I wouldn’t” (Hills, 1999a, p. 1B).

Liu and five of his Chinese coworkers “flunked lie-detector tests in which they asked if they had provided the passwords to anyone, downloaded the password files to steal them for personal gain, or used the passwords files to gain access to other computer systems” (Hills, 1999a, p. 1B). He also admitted in court that he knew that people from his country “should not have been allowed to work on the system: security was so lax, he concluded ‘was not a concern here’” (Hills, 1999a, p. 1B).

Socio-Economic Factors

As mentioned in Chapter Four, trends in the national and global environments impact the outsourcing market and its subsequent injections into an organization’s boundaries. One of those trends prevalent in today’s information technology defined culture is internationalization of IT jobs, within the United States and overseas.

Outsourcing Trends - International IT

Zhangyi Liu was one of 11 computer experts of Chinese nationality brought from Shanghai Tandem Software Systems, Ltd. from Shanghai, China in 1996. Offshore software development has been a building trend since the early 1990's, primarily due to cost (Mohan, 2001). The H1B visa program was part of this initiative to bring new talent into the IT development scene, as American workers were becoming reportedly scarce. This can be viewed from a social and cultural perspective as a way of "leveraging the creative talents of skilled workers around the globe" (Mohan, 2001, p. 103).

However, this may increase the insider threat if employees are from countries known to be conducting espionage activities against the United States. In Liu's case, China is a known intelligence threat to the U.S., and Liu was in a position to devastate a database critical to combat readiness status of the entire Air Force aircraft inventory.

Information Distribution

With geographical boundaries disintegrating into the IT global culture, unauthorized access within the bounds of the system can be easily exploited over the Internet to anyone outside the system. Liu's unauthorized access made sensitive file information completely visible over the Internet, which could have easily been exploited by China or any other foreign power (Hills and Gaffney, 1997b). Liu's case demonstrates a double-edged insider threat: the prolific distribution of information has the power to enable one trusted insider to unlock virtual doors (by installing backdoors, for example) for many outsiders.

Anti-American Sentiment

It was never released whether Liu had succeeded in making REMIS information available to Chinese adversaries, and two of Liu's Chinese coworkers have since returned to China. However, China's spying on the U.S. was at the forefront of the intelligence community during the Liu investigation, due to the investigation of Wen Ho Lee and his alleged theft of nuclear secrets from Los Alamos Laboratories. While no visible anti-Americanism was evident in Liu's case, it is becoming increasingly important to realize the unfortunate but critical threat potential from the international community.

During the presently on-going Global War on Terror, the FBI has communicated a serious threat from foreign intelligence services "who are dedicated to using any means necessary to obtain strategic information from the United States" (FBI, 2003, p. 9).

The Final Systemic Frontier – Security and Access Control

The IT Outsourcing and Insider Threat model depicts a logical relationship how factors and conditions outside an organization's boundaries inevitably impact the systemic conditions. While the physical layout of model constructs was intended to show merely interrelationships, it was surprising how the image of the model gives the impression of an arrow – pointing toward the Systemic Condition construct. This is where the insider works. The manager responsible for the information system, its people, security policies, practices, and access controls has a lot of issues and challenges in trying to control his information domain within seemingly diminishing borders.

Liu's case shows the need for access controls is detrimentally clear. The REMIS system was not secured with the intended security program that was designed to encrypt

user accounts and passwords (Hills and Gaffney, 1997). Furthermore, Liu was allegedly never given clear-cut security guidelines for what he could or could not do on the system. Finally, foreign nationals working on government IT systems has got to set off alarms with management in terms of threat potential, especially in an age increasing Anti-Americanism globally.

Implications

Liu was hired by XYPRO Technology Corporation in Simi Vally, California, the designer of the security system that was supposed to be installed on the REMIS system. Liu, however, "is no longer allowed to perform services for the [U.S.] government" (Hills, 1998, p. 2B). However, with increasing outsourcing trends in IT, how will the government know if he performs subcontractor services in the future? The need to aggressively track insider cases and monitor contractor behavior has been identified and made more urgent by the following statement during Robert Mueller, III's testimony before the Senate Select Committee on Intelligence on War on Terrorism:

> The government currently supports research and development in a large number of agencies, in a great many locations, many of which involve the use of thousands of government contractors. The FBI has the responsibility to assess the threat against those projects and to initiate operations that are directed at countering the threat. US Government entities, primarily the Departments of Energy and Defense, constitute the primary focus of the FBI's activity in this area. The individuals awarded research and development contracts in support of ongoing operations and war-making capabilities constitute the highest risk. (FBI, 2003, p. 9)

Summary

The Liu case is just one that implies the multi-dimensional threat from the inside is not a computer problem. It is truly a people problem. The model in Chapter Four demonstrates the dire complexities involved in outsourcing information technology that ultimately enables more outsiders to become insiders. The challenge for IT managers is tremendous, and it comes down to one thing – securing information from exploitation by the ill-meaning insider.

VI. Conclusion

Introduction

The insider threat is inherent in society's strive toward finding better, faster, cheaper, and simpler ways to pass information, accomplish business objectives, and survive in a fast-paced instant and impatient society. The risks have been created along with the technology, perhaps without fully realizing their devastating potential; or maybe we have just accepted the risks as part of technological advancement.

Regardless, it is clear that the insider threats and other security challenges were not created by the actual computers and technology, but by the people who have access, authorized or not, to the systems.

Findings

The most profound discovery of this research is the impact technology has had not only on how we do business, but how it has imposed social and psychological and even cultural metamorphoses on the last generation, if not last several generations. While evolutionary shifts in economies, markets, and even some aspects of cultures are natural, the last few decades have brought about permutations in society and our psyches for which rapid innovations may not have prepared us.

This research generated a comprehensive model that, through integration of concepts put forth in related literature and studies, presents a multidimensional view of

the scope of conditions from which the insider threat has emerged. It is a real, growing, and considerably urgent threat to information systems.

The emphasis on the model is the discursive nature of the insider threat in the outsourced IT environment. This threat cannot be confined to a static formula to calculate generic risk. It is operative and persevering, and needs to be dynamically measured, investigated, and reevaluated as social, economic, cultural, and technological trends shift. By following a contingency theory approach toward making this model modifiable to different situations where outsourcing is being considered, it may be possible to reduce or nearly eliminate some sources of threat when conscientiously applied.

However, the main focus of the theories and model generated by this research was to alter the decisional paradigm surrounding the outsourcing of IT and the threats that are possible. This model combines varied fields of study to assist decision-makers in transcending the bounded rationality that is human nature. While it is impossible to predict every source, method, motive, and timing of attacks, this model will aid in the protection of information systems from a wider range of scenarios, evident in recent insider attack events.

Implications

The thrust of this research was to not only raise awareness to the insider threat problem as it relates to outsourcing of information technology-based systems, but to encourage development of more comprehensive operational and personnel security programs focused on access to information. Where national security is concerned, there

should be more focus on the potential threats from internal sources, especially as outsourcing continues to increase as a way of doing business.

Today's outsourcing trend in military IT must build in better screening procedures. Tracking of personnel having access to critical systems "as perpetrators migrate from job to job, protected by the lack of background checks, constraints upon employers in providing references, and the lack of significant consequences for these offenses" (Shaw et al., 1998, p. 2) is crucial.

Recommendations for Further Research

The limitations of this research (lack of statistical data and metrics) offer significant opportunities for further research. While this is a new research area with no formal theory, additional research on the model presented in this thesis will allow for greater conceptual density.

This model gives a broad framework from which to analyze existing cases to determine the presence of conditions under which the insider is able to successfully carry out deviant actions. These actions could range from disregarding basic stated security policies (loyalty, ethical flexibility, personnel security practices, access, personality traits, uncertainty about future employment, length of employment, or triggers) to espionage activity (internationalization, interpersonal social frustrations, transactional behavior, access, outsourcing trends, opportunistic behavior, and ethical flexibility).

This model is presented for further research into the perceived rise in insider threat trends, and whether outsourcing of information technology is a major contributor to this problem. It was demonstrated that information technology is indeed not just a

service or administrative function to be contracted out to the lowest bidder. Current events give chilling examples daily of insiders endangering the security and lives of innocent people, and in order to protect them, it is vital to protect the information that is critical to national interests.

This model gives justification for further investigation of contracted (and subcontracted) information technology, especially in the Department of Defense. The clearance procedures of those entrusted to provide their valued services, the verification of the identities of all who access our information, and tracking of negative contractor (and others') behaviors should be a primary security consideration.

To reiterate concerns of the Insider Threat Integrated Process Team, "The Department [of Defense] has no unified database of insider case studies, lessons learned, physiological profiles or statistics regarding the insider and insider misuse, abuse, or malicious activity" (2000, p. A-2). Such a database urgently needs to built and utilized to obtain metrics on such activity.

A recommendation for further inductive research efforts to complete the theoretical density of this proposed model is to examine the social theories of outsourcing, such as social exchange, social contract, and power political theories. These theories will give even more social and psychological insight into outsourcing behaviors and conditions.

A final recommendation is to add a legal perspective to this model. A study of U.S. Codes, laws, and DoD Directives, and Federal Acquisition Regulations pertaining to information technology and security would be beneficial to determine whether legal protections or shortfalls are contributors to the insider threat to outsourced IT.

Recommendations to policy makers, based on potential relevant findings, could have national security implications in the future.

Conclusion

In reflecting back to this time 12 years ago, another George Bush was president, and we were building up forces for a pending conflict with Iraq. We were doing it without the extensive use of e-mail and the Internet, and with a military force twice as large and a force to be reckoned with (which is still the case) worldwide. Today, in the information age that was supposed to bring the world together through a global market, the United States has not only been attacked, but has been alerted to a clear and present danger of more devastating attacks - within the very borders we've opened to the world.

In trying to maintain proficiency in the rapidly changing information technology age, we've found it necessary to seek sources outside our organizational borders to keep up with societal and economic trends. In doing this, we've also opened our information to increased risks, not just from the outside, but from those we have trusted to manage the information this country trusts is in secure hands.

Notably, security vulnerabilities exposed by the events following the attacks on the United States on September 11th 2001 render this a timely topic that must bring information security to the forefront of our policy and processes. Former NIPC director Michael A. Vatis, in *Cyber attacks during the war on terrorism: A predictive analysis*, points out:

> Malicious insiders are the greatest threat to our critical national infrastructures. Insiders armed with specialized knowledge of systems and privileged access are capable of doing great harm. The tragedy of September 11, 2001 illustrates that

> terrorists live and operated within the United States, obtaining specialized skills with deadly intentions. (Vatis, 2001, p. 18)

Today's news is rampant with headlines featuring discoveries of trusted insiders stealing information, entire hard drives, committing espionage, sabotage, and other deceptive behaviors. Self-interest, broken loyalties, flexibility in moral and ethical decisions, and revenge are only a few of the exhibited motives. As cultural and societal shifts guide the shape of information value and distribution, management must be prepared to change its approach to securing the information and systems trusted to those on the inside.

A grave consideration must remain at the forefront of today's IT outsourcing decisions:

> "The nation's Critical National Assets are those persons, information, assets, activity, R&D technology, infrastructure, economic security or interests whose compromise will damage the survival of the United States."
>
> (Robert Mueller, III, 2003)

Bibliography

Air Force Doctrine Document (AFDD)-1. (1997). *Air Force Basic Doctrine.* Washington, DC: Department of Defense.

Al-Ayat, R.A., Judd, B.R., and Renis, T.A. (1986). The Safeguards Evaluation Method for Evaluating Vulnerability to Insider Threats, *Journal of the Institute of Nuclear Materials Management, Annual Meeting Proceedings, 15,* (27), 676-680.

Anderson, R.H., Bozek, T., Longstaff, T., Meitzler, W., Skroch, M., and Van Wyk, K. (2000). *Research on Mitigating the Insider Threat to Information Systems - #2: Proceedings of a Workshop Held August, 2000.* Retrieved July 17, 2002, from http://www.rand.org/publications/CF/CF163.

Antonucci, Y.L., Lordi, F.C., and Tucker, J.J., III. (1998). The Pros and Cons of Outsourcing, *Journal of Accountancy, 185,* (6), 26-38.

Cheon, M.J., Grover, V., and Teng, J.T.C. (1995). Theoretical Perspectives on the Outsourcing of Information Systems, *Journal of Information Technology, 10,* 209-219.

Clark, T.D, Zmud, R.W., and McCray, G.E. (1995). The Outsourcing of Information Services: Transforming the nature of business in the information industry, *Journal of Information Technology, 10,* 221-237.

Claver, E., Llopis, J., Garcia, D., and Hipolito, M. (1998). Organizational Culture for Innovation and New Technological Behavior, *Journal of High Technology Management Research, 9,* (1), 55-69.

Clemons, E. and Reddi, S.P. (1993). The Impact of Information Technology on the Organization of Economic Activity: The "move to the middle" hypothesis, *Journal of Management Information Systems, 10,* (2), 9-36.

Defense Security Service (DSS): Mission Degradation? U.S. Congressional Hearing by Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform, House of Representatives, 107th Congress, 13 (2001).

Denning, D.E. (1999). *Information Warfare and Security.* Reading, MA: ACM Press.

DoD Security Review Commission. *Keeping the Nation's Secrets: A report to the Secretary of Defense by the commission to review DoD security policy and practices,* 1985.

Drucker, P. (1993). *Post Capitalist Society.* New York, NY: HarperCollins.

Domberger, S., Fernandez, P., and Fiebig, D.G. (2000). Modelling the Price, Performance, and Contract Characteristics of IT Outsourcing, *Journal of Information Technology, 15,* 107-118.

Executive Order 13010 (1996). Executive Order 13010-Critical Infrastructure Protection, *Federal Register, 61,* (138), 37345-37350.

Federal Bureau of Investigation (FBI). (1998). *Statement for the Record of Louis J. Freeh, Director, FBI, on Threats to U.S. National Security, Before the Senate Select Committee on Intelligence*. Washington, D.C: Freeh, L. J.

Federal Bureau of Investigation (FBI). (2000). *Statement for the Record of Louis J. Freeh, Director, FBI, on Cybercrime, Before the Senate Committee on Judiciary Subcommittee for Technology, Terrorism, and Government Information*. Washington, D.C: Freeh, L. J.

Federal Bureau of Investigation (FBI). (2003). *Statement for the Record Robert S. Mueller, III, Director, FBI, on War on Terrorism, Before the Senate Select Committee Intelligence*. Washington, D.C: Mueller, R.S.III.

Fink, D. (1994). A Security Framework for Information Systems Outsourcing. *Information Management and Computer Security, 2,* (4), 3-8.

Gaffney, T.R. (1997, June 15). Computer Hacker – File Found During Cleanup. *Dayton Daily News,* p. 19A.

Glaser, B.G. (1992). *Basics of Grounded Theory Analysis.* Mill Valley, CA: Sociology Press.

Glaser B.G. (1998). *Doing Grounded Theory: Issues and Discussions.* Mill Valley, CA: Sociology Press.

Glaser B.G. and Strauss, A.L. (1967). *The Discovery of Grounded Theory.* Chicago, IL: Aldine Publishing Co.

Grover, V. and Ramanlal, P. (1999). Six Myths of Information and Markets: Information technology networks, electronic commerce, and the battle for consumer surplus, *MIS Quarterly, 23,* (4), 465-495.

Hills, W. (1997, December 12). Hearing Spells out Threat. *Dayton Daily News*, p. 1A.

Hills, W. (1998, May 23). Hacker Set to Work for Computer Firm. *Dayton Daily News*, p. 2B.

Hills, W. (1999, April 11). Security Breach Penalty Stuns AF. *Dayton Daily News*, p. 1B.

Hills, W. (1999, October 21). AF Hacker on the Other Side of the Fence. *Dayton Daily News*, p. 1A.

Hills, W. (2000, January 13). Chinese National Faces Harsher Sentence. *Dayton Daily News*, p. 1B.

Hills, W. (2000, January 15). Chinese National Gets Sentence of 4 Months. *Dayton Daily News*, p. 3B.

Hills, W. and Gaffney, T.R. (1997, June 15). AF Computer Security Lax Chinese Worker Gained Access. *Dayton Daily News*, p. 3B.

Hills, W. and Gaffney, T.R. (1997, November 10). AF Computers – Service Fears Bugs Planted. *Dayton Daily News*, p. 1A.

Heuer, R.J., Jr. (1999). *The Changing Environment for the National Industrial Security Program: Implications and issues*, Defense Security Service, Security Research Center. PERSEREC: Monterey, CA.

Heuer, R. J., Jr. (2001). *The insider espionage threat*. Retrieved 12 July 2002, from http://www.smdc.army.mil/SecurityGuide/Treason/Insider.htm.

Hodson, R. and Sullivan T.A. (1985). Totem or Tyrant? Monopoly, regional, and local sector effects on worker commitment, *Social Forces*, *63*, (3), 716-731.

Insider Threat Integrated Process Team (IPT). (2000). *DoD Insider Threat Mitigation: Final report of the insider threat integrated process team, April 24, 2000*.

Joint Security Commission. (1994). *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence, February 28, 1994.* Washington, DC: GPO. Retrieved May 4, 2002, http://www.fas.org/sgp/library/jsc

Jurison, J. (1995). The Role of Risk and Return on Information Technology Outsourcing Decisions, *Journal of Information Technology*, *10*, 239-247.

Keeler, A.G. (1997). *Third World Computer Systems: A Threat to the security of the United States?* (Air Command and Staff College Rep. No. AU/ACSC/97-0603/97-03).

Keough, H.R. (1989). An Inside Job, *Security Management, 33,* (2), 13A-16A.

Kliem, R. (1999). Managing the Risks of Outsourcing Agreements, *Information Systems Management, 16,* (3), 91-94.

Klepper, R. and Jones, W.O. (1998). *Outsourcing Information Technology Systems and Services.* Upper Saddle River, NJ: Prentice Hall.

Lacity, M. and Hirschheim, R. (1994). Realizing Outsourcing Expectations, *Information Systems Management, 11,* (4), 7-21.

Lacity, M., Willcocks, L.P., and Feeny, D.F. (1995). IT Outsourcing: Maximize flexibility and control, *Harvard Business Review,* May-June, 84-93.

Lee, J. N. and Kim, Y.G. (1999). Effect of Partnership Quality on IS Outsourcing Success: Conceptual framework and empirical validation, *Journal of Management Information Systems, 15,* (4) 29-64.

Levina, N. (1999). *Sources of Vendor Production Cost Advantages in IT Outsourcing* (CISR Working Paper (WP) No. 309, Sloan WP No. 4094). Cambridge, MA: Massachusetts Institute of Technology, Center for Information Systems Research (CISR).

Loch, K.D. and Carr, H.H. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding, *MIS Quarterly, 16,* (2), 173-192.

Lunney, K. (May 7, 2002). Watchdog group calls for better oversight of contractors. *GovExec.com.* Retrieved May 16, 2002, from http://www.govexec.com/dailyfed/0502/050702.

Magklaras, G.B. and Furnell, S.M. (2002). Insider Threat Prediction Tool: Evaluating the probability of IT misuse, *Computers and Security, 21,* (1), 62-73.

Marshall, C. and Rossman, G. (1989). *Designing Qualitative Research.* Newbury Park, CA: Sage Publications

Mata, F.J. and Fuerst, W.L. (1995). Information Technology and Sustained Competitive Advantage: A resource-based analysis, *MIS Quarterly, 19,* (4), 487-507.

Modic, R. (1999, July 7). Chinese Programmer Copied Secret Code List. *Dayton Daily News,* p. 2B.

Modic, R. (1999, July 9). Metro Programmer Convicted. *Dayton Daily News,* p. 1B.

Mohan, K. (2001). The International Software Connection, *IEEE Software, 18,* (1), 100-103).

McNulty, P.J. (2002). Superceding Indictment of Brian Regan. Retrieved July 17, 2002, from http://intellit.muskingum.edu/spycases_folder/spycasesustoc.html.

Mueller, C.W. and Wallace, J.E. (1992). Employee Commitment, *Work and Occupations, 19,* (3), 211-238.

National Aeronautics and Space Administration (NASA) Office of Inspector General (2001). *Semiannual Report to Congress, October 1, 2000-March 31, 2001.* Retrieved February 2, 2003, from http://demilo.public.hq.nasa.gov/office/oig/hq/sar0301.pdf.

National Aeronautics and Space Administration (NASA) Office of Inspector General (2002). *Semiannual Report to Congress, October 1, 2001-March 31, 2002.* Retrieved February 2, 2003, from http://demilo.public.hq.nasa.gov/office/oig/hq/sar033102.pdf

National Communications System (NCS), Office of the Manager. (2000). *The Electronic Intrusion Threat to National Security and Emergency Preparedness (NS/EP) Internet Communications: An awareness document*. Retrieved on 14 March, 2002, from http://www.ncs.gov/ncs/Reports/electronic_intrusion_threat2000_final2.pdf

National Counterintelligence Center (NACIC). (1996). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage.* Retrieved on 14 March, 2002 from http://www.fas.org/irp/ops/ci/docs/fy96.htm

National Counterintelligence Center (NACIC). (2000). *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*. Retrieved June 16, 2002 from http://www.iwar.org.uk/ecoespionage/resources/senate/annual-reports/industrial-espionage-00.htm

National Infrastructure Protection Center (NIPC). (1999). *NIPC Cyber Threat Assessment - 6 October 1999 (Statement for the Record of Michael A. Vatis, Director, National Infrastructure Protection Center, Federal Bureau of Investigation, before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism).*

National Security Telecommunications and Information Systems Security Committee (NSTISSC). (1999). *The Insider Threat to U.S. Government Information Systems* (Report No. NTISSAM INFOSEC/1-99). Fort Meade, MD: NTISSC Secretariat.

Office of Management and Budget (OMB). (2001). *FY 2001 Report to Congress on Federal Government Information Security Reform*. Washington, DC: GPO.

Office of Management and Budget (OMB). (1999). *Performance of Commercial Activities.* (OMB Circular No. A-76). Washington, DC: GPO.

Office of Management and Budget. (OMB). (2002). *Budget of the United State s Government, FY 2003, MSR, Progress Implementing the President's Management Agenda* (Report No. OMB/MSR-06). Washington, DC: GPO. July 17, 2002, from http://www.whitehouse.gov/omb/budget/fy2003/msr06.html

Peckenpaugh, J. (June 25, 2001). When FAIR is fair. *GovExec.com.* Retrieved February 21, 2002, from http://www.govexec.com/news/index.cfm

Peckenpaugh, J. (January 11, 2002). Pentagon wants out of OMB competitive sourcing plan. *GovExec.com.* Retrieved February 21, 2002, from http://www.govexec.com/news/index.cfm

Peters, K.M. (April 1, 1999). Information Insecurity. *GovExec.com.* Retrieved February 21, 2002, from http://www.govexec.com/news/index.cfm

Pew Research Center (2002). *What the World Thinks in 2002: How the global publics view: their lives, their countries, the world, America.* Washington, DC: The Pew Research Center for the People and the Press. Retrieved February 5, 2002 from http://people-press.org/reports/files/report165.pdf

Power R. (2002). 2002 CSI/FBI Computer Crime and Security Survey. *Computer Security Institute.* Retrieved 14 July 02 from http://www.gocsi.com/pdfs/fbi/FBI2002.pdf

Poulsen, K. (January 16, 2003). Rumsfeld Orders .mil Web Lockdown. *Security Focus Online.* Retrieved January 21, 2003, from http://online.secuityfocus.com/news/2062.

Project on Government Oversight (POGO) (May 10, 2002). *Federal Contractor Misconduct: Failures of the suspension and debarment system.* Retrieved May 15, 2002, from http://www.pogo.org/p/contracts/co-020505-contractors.html.

Quinn, E.A. (1983). Insider Threat – NRC's Perspective, *Journal of the Institute of Nuclear Materials Management, Annual Meeting Proceedings, 12*, 85-86.

Ruber, P. (2000, November 27). The Great IT Foreign Worker Debate. *Information Week.com.* Retrieved January 13, 2003, from http://www.informationweek.com/814/visas.htm

Rumsfeld, D. H. (2002). *Annual Report to the President and the Congress.* Washington, DC: GPO.

Sambamurthy, V. and Zmud, R.W. (2000). The Organizing Logic for an Enterprise's IT Activities in the Digital Era: A prognosis of practice and a call for research, *Information Systems Research, 11,* (12), 105-115.

Schein, E.H. (1985). *Organizational Culture and Leadershi*p, Jossey-Bass Press, San Francisco.

Schultz, E.E. (2002). A Framework for Understanding and Predicting Insider Attacks, *Computers and Security, 21*, (6), 526-531.

Shaw, E.D., Ruby, K.G., and Post, J.M. (1998). The insider threat to information systems. *Security Awareness Bulletin, 2-98.* Department of Defense Security Institute.

Shaw, E.D., Ruby, K.G., and Post, J.M. (1999). Inside the mind of the insider, *Security Management, Dec 99.*

Schwartz, J. (2002, January 6). Experts See Vulnerability as Outsiders Code Software. *New York Times.* Retrieved January 6, 2002, from http://www.nytimes.com.

Sherwood, J. (1997). Managing Security for Outsourcing Contracts, *Computers and Security, 16,* (7), 603-609.

Slaughter, S. and Ang, S. (1996). Employment Outsourcing in Information Systems, *Communications of the ACM, 39,* (7), 47-54.

Strauss, A. (1987). *Qualitative Analysis for Social Scientists.* New York, NY: Cambridge University Press.

Strauss, A. and Corbin, J. (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques.* Newbury Park, CA: Sage Publications.

Sun, S.Y., Lin, T.C., and Sun, P.C. (2002). The Factors Influencing Information Systems Outsourcing Partnership – A Study Integrating Case Study and Survey Research Methods. *Proceedings of the 35th Hawaii International Conference on System Sciences – 2002, USA.*

Swartz, J. (2001, October 17). Tech-Visa Workers Feel Heat. *USA Today*. Retrieved January 13, 2003, from http://www.usatoday.com/money/covers/2001-10-17-bcovwed.htm.

Tayntor, C. B. (2001). A Practical Guide to Staff Augmentation and Outsourcing, *Information Technology, 18,* (1), 84-92.

United States General Accounting Office. (GAO). (1996). *Defense Industrial Security: Weaknesses in U.S. Security Arrangements With Foreign-Owned Defense Contractors* (Report No. GAO/NSIAD-96-94). Washington, DC: GPO

United States General Accounting Office. (GAO). (1998). *Information Security: Serious weaknesses place critical federal operation and assets at risk* (Report No. GAO/AIMD-98-92). Washington, DC: GPO.

United States General Accounting Office. (GAO). (2002). *Desktop Outsourcing: Positive results reported, but analyses could be strengthened* (Report No. GAO-02-329). Washington, DC: GPO.

U.S. Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, Information Warfare and Critical Infrasturcture Protection. (1999). *Statement by The Honorable Arthur L. Money, Senior Civilian Official, Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence and DoD Chief Information Officer.* Retrieved July 15, 2002 from http://www.c3i.osd.mil/org/pe/cd/testimony/sasciwcis031699.html.

Vatis, M. A. (2001). *Cyber Attacks During the War on Terrorism: A predictive analysis.* Hanover, NH: Institute for Security Technology Studies at Dartmouth College.

Willcocks, L.P. and Lacity, M.C. (1995). Information Outsourcing in Theory and Practice, *Journal of Information Technology, 10,* 203-207.

Zaiton, H. (2000). Insider Cyber Threats: Problems and Perspectives, *International Review of Law, Computers, and Technology, 14,* (1), 105-114.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
25-03-2003	**Master's Thesis**	Aug 2001 – Mar 2003

4. TITLE AND SUBTITLE

OUTSOURCING INFORMATION TECHNOLOGY AND THE INSIDER THREAT

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Caruso, Valerie L., 1st Lieutenant, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENG/03-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Personnel Security Research Center (PERSEREC)
Attn: Dr. Lynn Fischer
99 Pacific St., Building 455 E Comm: (831) 657-3005
Monterey, CA 93940-2481 e-mail: FischeLF@osd.pentagon.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT As one of our nation's top critical infrastructures, telecommunications is an essential element of many aspects of our lives upon which we, as a society, are becoming increasingly dependent. Computers, digital telephone switches, and interconnected information technology (IT) systems impact finances, travel, infrastructure management, and missions of national defense.

This research examined whether the trend in increased outsourcing of information technology systems is a significant contributing factor to a reportedly increasing amount of insider attacks. In light of changing social, global economic, and technological conditions, the paradigm in which risk analysis, management practices, and operational and personnel security practices are applied to protect information has shifted over the last decade.

A comprehensive model of the discursive nature of the insider threat in the outsourced IT environment was developed using a qualitative grounded theory approach put forth by Glaser and Strauss in 1967. The theory generated by this research suggests a multidimensional real and growing threat resulting from outsourced IT as well as preconditions for continued future growth of the insider threat phenomenon.

15. SUBJECT TERMS

Insider Threat, Outsourcing, Information Technology, Risk Assessment

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Gregg H. Gunsch, PhD, AFIT/ENG
U	U	U	UU	145	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-6565 x 4281 Gregg.gunsch@afit.edu